PROYECTO DE TRABAJO DE GRADO

GUÍA PARA LA IMPLEMENTACION DE LA NORMA ISO 27032.

SANDRA LILIANA GUZMÁN SOLANO

CODIGO: 63000109

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C JUNIO 2019

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

La seguridad informática busca garantizar la disponibilidad, integridad y confiabilidad de la información que se gestiona a través de medios tecnológicos, permitiendo un crecimiento en las organizaciones, fomentando la innovación y ventajas competitivas en el mercado que se desempeñan.

Sin embargo, es importante tener claro que no existen mecanismos, controles o herramientas que permitan tener la seguridad de la información en un 100%, garantizando la continuidad de los servicios y/o las operaciones críticas de las organizaciones.

Dado lo anterior surge este proyecto de investigación mediante el cual se pretende generar mecanismos para que las organizaciones puedan mitigar los riesgos y dar respuesta de manera oportuna a los incidentes informáticos. Para ello se tomará como base las buenas prácticas planteadas en la norma ISO 27032 con el fin de generar una guía que brinde a los encargados de TI, los lineamientos para identificar los riesgos a los cuales están expuestos de acuerdo a la información que tienen publicada en el ciberespacio y que puede llegar a afectar el objetivo del negocio, generando los controles necesarios a implementar de tal forma que aseguren de manera óptima los diferentes activos de información.

1 GENERALIDADES

1.1 LÍNEA DE INVESTIGACIÓN

Software Inteligente y Convergencia tecnológica.

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 ANTECEDENTES DEL PROBLEMA

En los últimos 3 años, las compañías en Colombia han venido creciendo en la implementación de tecnologías para el desarrollo de sus operaciones, con referencia a las PYMES su crecimiento se ha visto incrementado de acuerdo a lo identificado por el DANE en 2017[1], donde se observa el crecimiento en las conexiones a internet, la adquisición de servicios en la nube, así como la implementación de aplicaciones en línea para el desarrollo de sus actividades. Dado este crecimiento también se han incrementado los ataques informáticos como ingeniería social, denegación de servicio entre otros realizados por adolescentes a ataques que son ejecutados por redes profesionales con grandes ambiciones como hurto de propiedad intelectual o dinero entre otros, razón por la cual la Ciberseguridad ha adquirido un espacio importante para los empresarios dado el impacto que ha generado en diferentes industrias no solo en el país sino en el mundo.

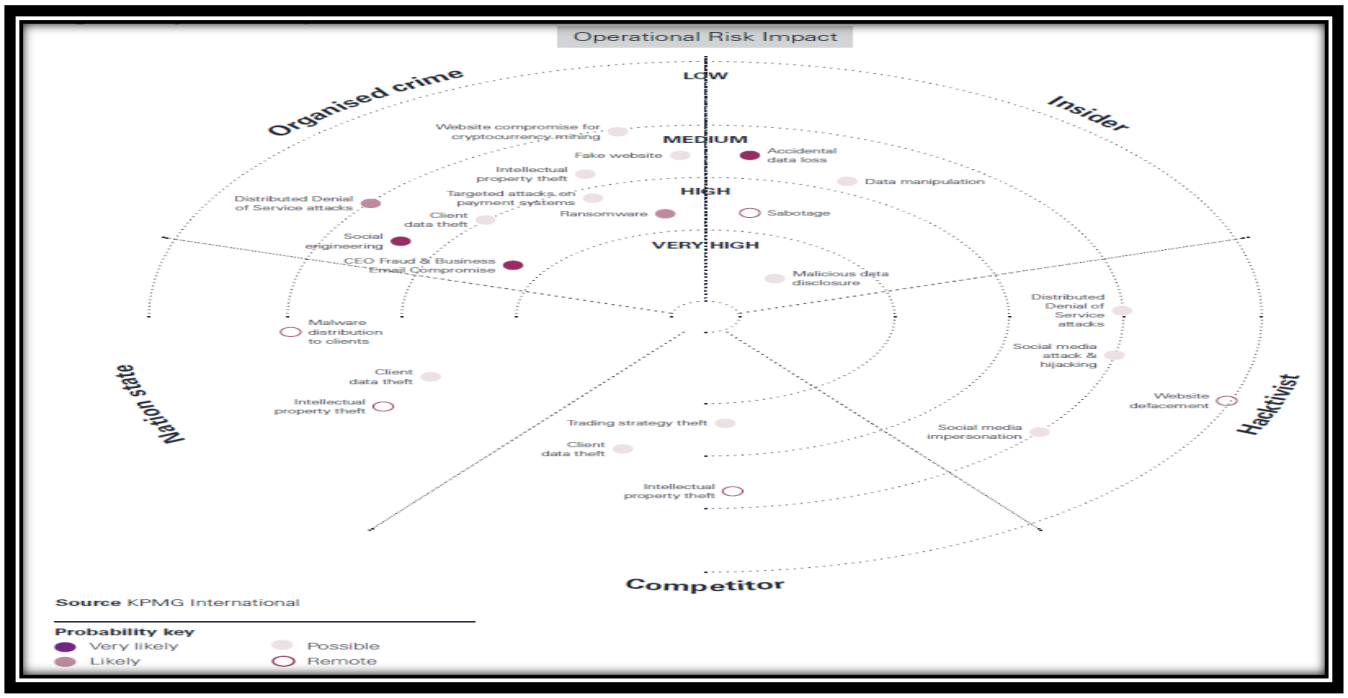
KPMG presentó (2018) el radar de riesgos de Ciberseguridad [2] el cual se pueden apreciar en la Figura 1, donde se observan los 5 actores de amenazas dentro de los cuales esta: el crimen organizado el cual no solo se presenta a nivel externo sino en que en muchas ocasiones este tipo de ataques vienen desde el interior de las organizaciones debido a que no hay una adecuada concientización frente a este

[1] Micrositios, Mintic. ABC de la digitalización (2017), http://micrositios.mintic.gov.co/abc_digitalizacion_empresas/.

[2] KPMG, (2018), Building Cyber Resilience in Asset Management, Thought Leadership, Cyber security risk radar https://assets.kp mg.com/content/dam/kpmg/bm/pdf/2018/07/building-cyber-resilience-in-asset-management.pdf

tipo de temas hacia los colaboradores independientemente del área o servicio que brindan, el siguiente son las personas interesadas o que cuentan con información privilegiada la cual en muchos casos no realizan el tratamiento o toman medidas de seguridad necesarias de acuerdo a la criticidad de la misma, impacto entre otros. Continuando con el radar se encuentran los Hacktivistas encargados de generar los ataques que afectan las organizaciones y de acuerdo al radar los riesgos son medios y altos para las organizaciones. Finalmente, como último actor se observa el Estado el cual en algunos países no cuenta con los lineamientos y/o controles necesarios que mitiguen riesgos a los cuales se ven expuestas las entidades estatales de los mismos y que a su vez brindan servicios a las diferentes organizaciones exponiéndose a riesgos de mayor impacto. [3]

Figura 1 - Cyber security risk radar

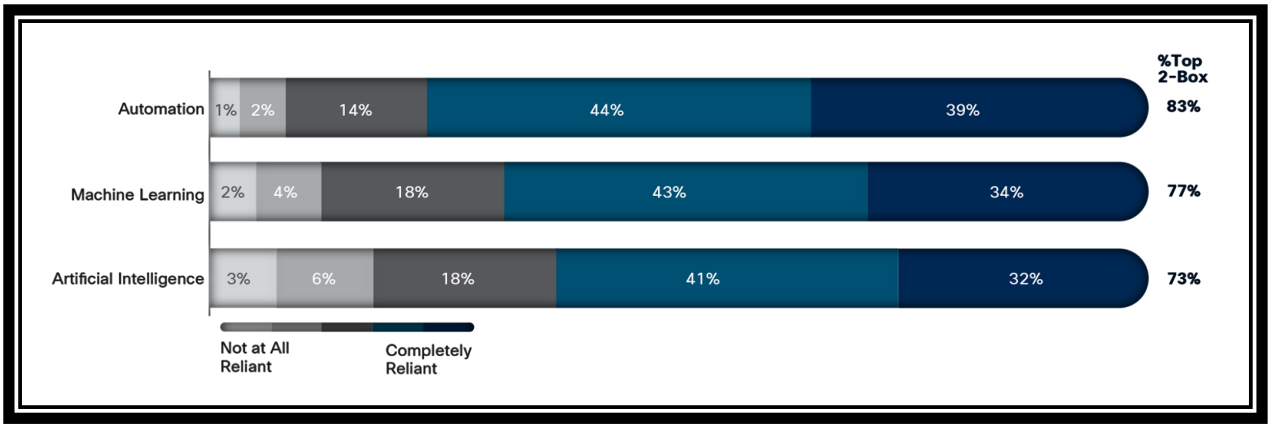


Fuente: Building Cyber Resilience in Asset Management – 2018, *https://intra.ema.kpmg.com/sites/SGI/CyberSecurity/Pages/GlobalCyberSecurityHome.aspx*

[3] KPMG, (2018), Building Cyber Resilience in Asset Management, Thought Leadership, Cyber security risk radar https://intra.ema.kpmg.com/sites/SGI/CyberSecurity/Lib01/01/Building_Cyber_Resilience_In_Asset_Management.PDF

Dentro de los estudios y/o encuestas de Ciberseguridad también existe el Reporte Anual de Ciberseguridad de Cisco 2018 en el cual se menciona la aparición de los cryptoworms ransomware basados en la red lo que ha eliminado la necesidad del elemento humano en el lanzamiento de este tipo de ataques[4], lo que ha permitido que estos se incrementen y a su vez no sean detectados de manera oportuna. Adicionalmente indagaron acerca de las capacidades de Seguridad con las que cuentan las Organizaciones evidenciando que entre un 30% a 44%, de acuerdo a lo que se observa en la Figura 2.

Figura 2 - Las organizaciones dependen en gran medida de la automatización, el aprendizaje de máquina y la inteligencia artificial



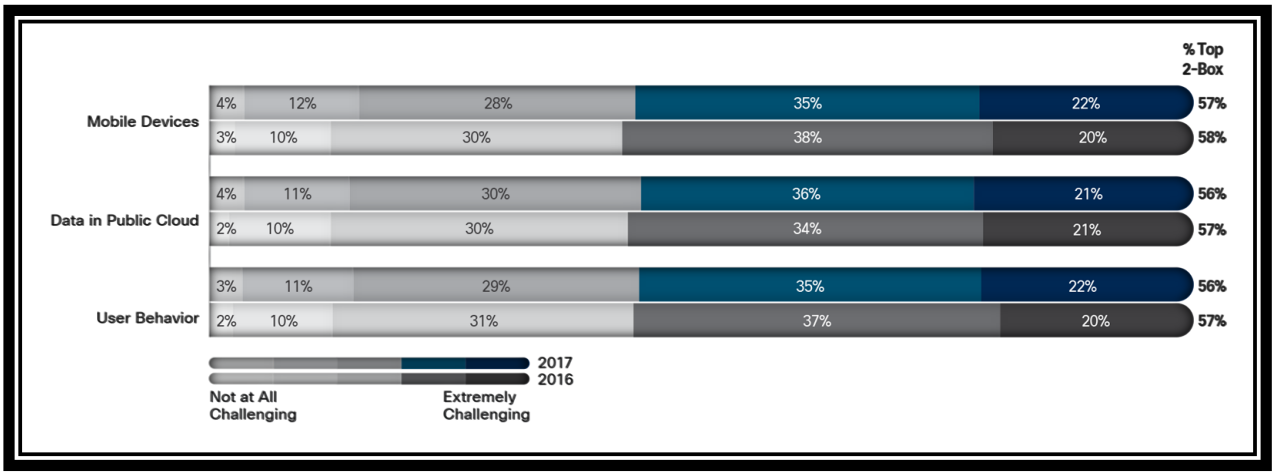
Fuente: Reporte anual de CISCO 2018, https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

La figura anterior ilustra lo importante que se ha convertido para las organizaciones la automatización, el aprendizaje de máquina y la inteligencia artificial para sus operaciones CORE, generando que estén más expuestos a ataques cibernéticos al no contar con controles efectivos que mitiguen estos riesgos.

[4] CISCO, 2018, Reporte Anual de Ciberseguridad de Cisco 2018 https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

Otro de los aspectos importantes que muestra el reporte de CISCO son los retos y obstáculos a los cuales se ven enfrentados los encargados de Seguridad en las organizaciones al momento de proteger las áreas o funciones claves de sus organizaciones, dado que ya no solo deben pensar en cómo proteger la infraestructura y/o información que reposa en ella para el desarrollo de las operaciones sino que también deben tener en cuenta el acceso que tienen a la información mediante dispositivos móviles así como el comportamiento, conocimiento y experticia que tienen los usuarios finales para el manejo de los datos y/o información que esta publicada en la nube, de acuerdo a lo que se observa en la Figura 3.

Figura 3 – Áreas más difíciles de defender.



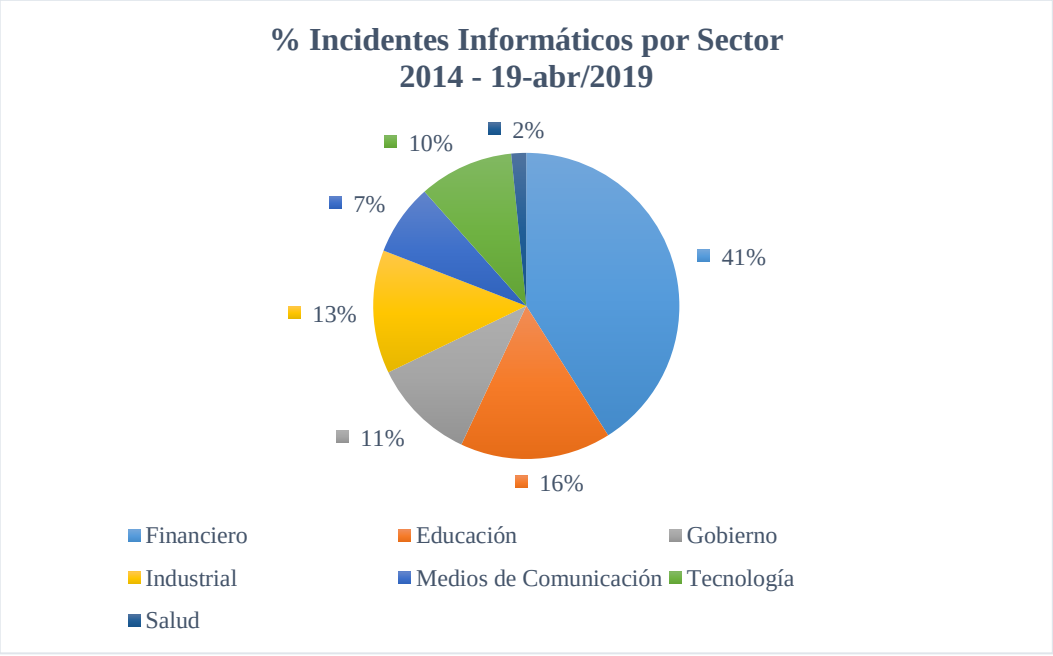
Fuente: Reporte anual de CISCO 2018, https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

En la figura 3 se observa el resultado de los aspectos críticos para las organizaciones donde han aumentado su uso entre 2016 y 2017, sin embargo solo para el 21% de las organizaciones evaluadas es extremadamente desafiante el manejo y administración de estos nuevos cambios, por lo que también se ha incrementado la necesidad de contar con expertos en seguridad que se encarguen de implementar

controles que mitiguen los riesgos a los cuales se ven expuestos con estos cambios tecnológicos tomando como factor crítico las personas.

A nivel de Colombia una de las entidades que atiende y monitorea los incidentes informáticos es la Policía Nacional desde su Centro Cibernético Policial - CCP[5], allí cuentan con estadísticas por sector y tipos de incidentes, mediante los cuales se puede evidenciar como han incrementado en el país los ataques informáticos, donde de acuerdo a las indagaciones con ellos Bogotá, Medellín y Cali son las ciudades donde más incidentes se presentan. A continuación en la Figura 4, se presenta el comportamiento por cada uno de los sectores, de acuerdo a las cifras suministradas por el CCP desde el año 2014 hasta el primer trimestre de 2019.

Figura 4 – Incidentes Informáticos por Sector.



Fuente: Estadísticas Centro Cibernético Policial

En la figura de incidentes se observa que el porcentaje más alto está en el sector financiero con un

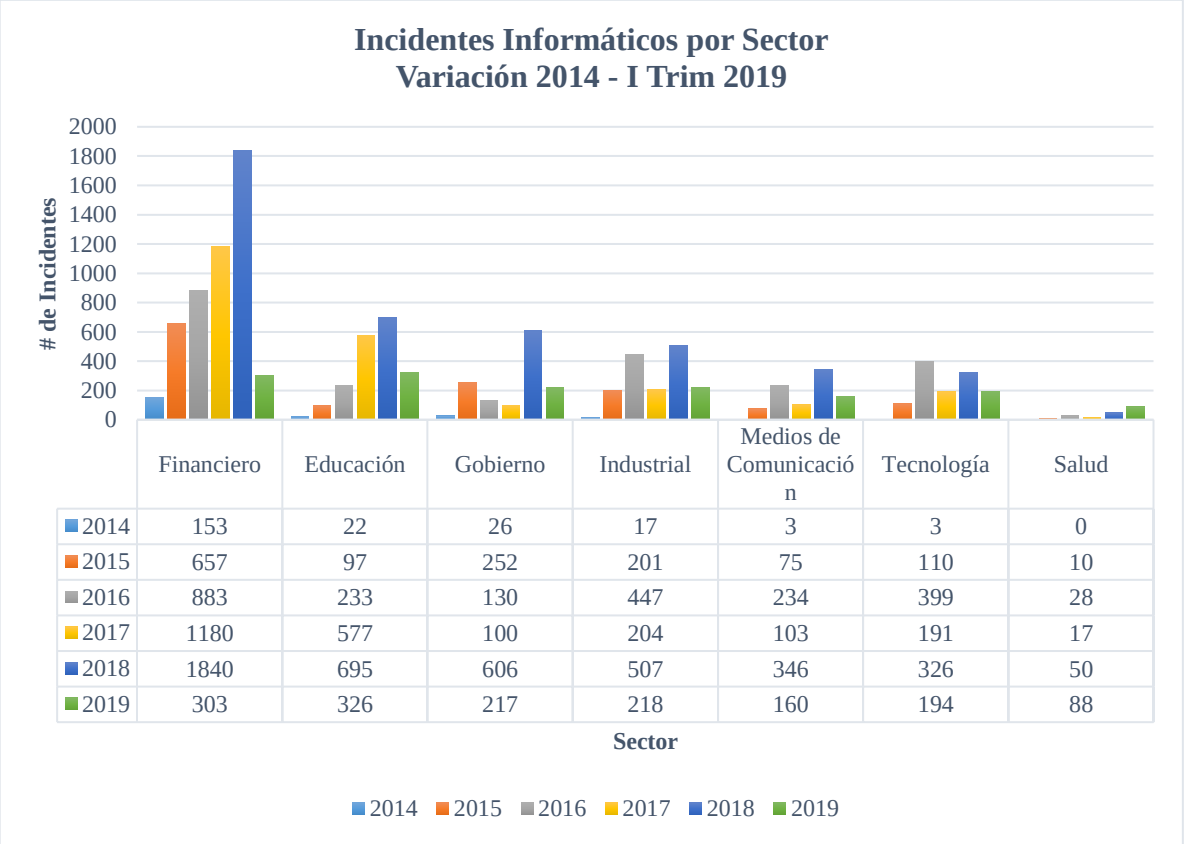
[5] Centro Cibernético Policial, 2019, Estadísticas Incidentes Informáticos 2014 – 2019 https://caivirtual.policia.gov.co/

46% y el más bajo se ubica en el sector de la Salud con un 2%, lo que evidencia que el sector Financiero al ser un sector que ha tenido cambios importantes con la implementación de herramientas y/o transformación de su modelo de servicios pasado de un esquema presencial a un esquema virtual y contar con regulaciones que garanticen controles para mitigar riesgos que impacten sus operación, ha faltado una cultura digital hacia los usuarios finales donde ellos entiendan la importancia del buen uso de estos mecanismos.

En la

Figura 5 se observa el comportamiento de los incidentes en cada sector para el periodo 2014 hasta el primer trimestre de 2019, evidenciando un crecimiento proporcional a su transformación digital.

Figura 5 – Variación Incidentes Informáticos por Sector.



	Financiero	Educación	Gobierno	Industrial	Medios de Comunicación	Tecnología	Salud
2014	153	22	26	17	3	3	0
2015	657	97	252	201	75	110	10
2016	883	233	130	447	234	399	28
2017	1180	577	100	204	103	191	17
2018	1840	695	606	507	346	326	50
2019	303	326	217	218	160	194	88

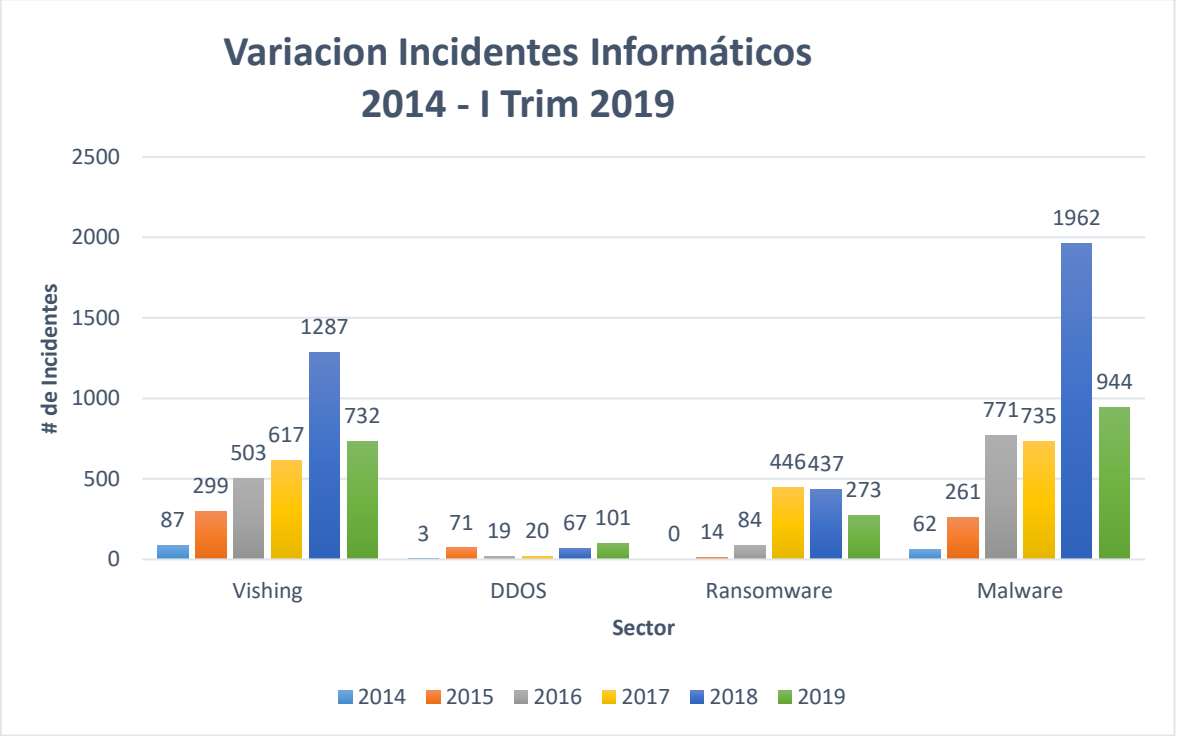
Fuente: Estadísticas Centro Cibernético Policial

Nuevamente se observa que el sector más atacado por los Ciberdelincuentes es el Financiero, a

pesar de ser uno de los más regulados y monitoreados por entes como la Superfinanciera y Asobancaria respectivamente, mientras que sectores como el de la Salud que hasta el momento está incursionando en la transformación digital es uno de los menos afectados por la ciberdelincuencia.

Otro de los informes suministrados por el CCP es el que se muestra en la *Figura 6*, que hace referencia a los principales ataques, sobre los cuales reciben reportes.

Figura 6 – Variación Incidentes Informáticos.



Fuente: Estadísticas Centro Cibernético Policial

En la figura anterior se puede evidenciar que el malware y el vishing son los incidentes que más se han incrementado en Colombia, presentando un crecimiento significativo en el año 2018, mientras que ataques como el DDOS, han disminuido, luego de que durante décadas fuera el principal riesgo para las Compañías, lo cual permite inferir que a medida que se generan cambios en las tecnologías aumentan los mecanismos de ataque utilizados por los ciberatacantes.

1.2.2 PREGUNTA DE INVESTIGACIÓN

¿Cómo preparar a las Organizaciones para mitigar los riesgos y responder de manera oportuna a los incidentes de Ciberseguridad de acuerdo con la norma ISO 27032?

1.2.3 VARIABLES DEL PROBLEMA

Personas: Cada una de las personas que hacen uso de las nuevas tecnologías o han incursionado en la transformación digital de los diferentes sectores.

Activos de información: Son todos los recursos (Personas, sistemas, Equipos de Cómputo, Bases de datos, entre otros) que tienen valor para la organización y mediante los cuales la misma puede desarrollar sus operaciones.

Ciberespacio: Espacio virtual donde las organizaciones están almacenando la información de sus operaciones o procesos.

Capacitación: Mecanismos que son utilizados por las organizaciones u entidades para dar a conocer un tema de interés para un grupo de personas en particular.

1.3 JUSTIFICACIÓN

A medida que la tecnología y la seguridad de la información evolucionan, también lo hacen a gran escala los ataques en el ciberespacio, generando que el mundo cibernético se convierta en un tema importante y en algunas ocasiones crítico para las juntas directivas y altas gerencias de las diferentes organizaciones sin importar su tamaño o tipo de negocio. Es por esto que con el proyecto se quiere contribuir a identificar el nivel de preparación de la compañías para mitigar o responder a eventuales incidentes informáticos, proporcionando una guía con los lineamientos a tener en cuenta para implementar buenas prácticas que les permita actuar de manera oportuna y eficientemente ante un ciberataque, los cuales son difíciles de predecir, pero una organización debe prepararse para tomar acciones frente a los riesgos a los cuales se ven expuestas, iniciando por el activo más crítico y vulnerable que como es el recurso humano, dado que a pesar de que las adquieren herramientas e implementar controles para mitigar riesgos, en algunos casos los funcionarios no cuentan con capacitación y/o concientización que les permita identificar amenazas a las cuales exponen la información y/o recursos que utilizan para sus labores diaria, posteriormente deben enfocarse en las aplicaciones y/o información que está alojada en ambientes del ciberespacio o en la infraestructura que no es directamente administrada por ellos sino por terceros, estas situaciones hace que requieran contar con expertos los cuales tengan los conocimientos necesarios para la implementación de controles efectivos que contribuyan a minimizar el impacto que pueda generar este tipo de situaciones. Es por ello que nace la necesidad de generar una guía para la implementación de las buenas prácticas que se plantean en la norma ISO 27032, la cual les permite a las organizaciones identificar, analizar y establecer controles que contribuyan a fortalecer los niveles de seguridad para mitigar los riesgos a los cuales se ven expuestos en el ciberespacio.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Diseñar una guía para la implementación de las buenas prácticas de la norma ISO 27032 estableciendo los requerimientos necesarios para adoptarlas en las organizaciones, de tal forma que cuenten con mecanismos que les permita identificar los riesgos a los que se ven expuestos la información en el ciberespacio y que pueden llegar a afectar la continuidad de su operación.

1.4.2 OBJETIVOS ESPECÍFICOS

- Identificar las buenas prácticas de Ciberseguridad en las organizaciones de acuerdo a los requerimientos establecidos en la norma ISO27032.
- Definir criterios para evaluar la implementación de las buenas prácticas de Ciberseguridad en las organizaciones de acuerdo a la norma ISO 27032.
- Establecer los lineamientos para implementar los controles y hacer seguimiento a la implementación de las buenas prácticas de Ciberseguridad de acuerdo a la norma ISO 27032.

2 MARCOS DE REFERENCIA

2.1 MARCO CONCEPTUAL

Las siguientes definiciones fueron tomadas de los libros: Seguridad en Equipos informáticos[6] y Como Implantar un SGSI[7]

SGSI: Es un conjunto de procesos que comprende las políticas, estructura organizativa, los recursos, procedimientos, procesos necesarios para implementar y mejorar de manera continua la Seguridad de la Información tomando como base los riesgos a los cuales se enfrentan la organización.

Ciberseguridad: Es la disciplina que se encarga de aplicar diferentes medidas de seguridad (tecnológicas principalmente, pero también organizativas, contractuales, operativas o normativas) para proteger los activos de una organización de las amenazas provenientes del ciberespacio.

Seguridad de la información: Es el conjunto de medidas y procedimientos que permiten proteger la integridad, disponibilidad y confidencialidad de la información.

Activo: Todo aquello que tenga valor (Sistema, información, personas, otro) y deba ser protegido frente a un ataques o afectación intencionada o no

Vulnerabilidades: Son las debilidades detectadas en un activo que puedan afectar el funcionamiento de los sistemas de la información de las organizaciones.

Ataques: Son las acciones mediante las cuales terceros aprovechan las vulnerabilidades de los sistemas

[6] Gomez Vietes, Álvaro, Ed 1, 2013, Seguridad en Equipos Informáticos, Bogotá, Colombia, Ediciones de la U.
[7] Gómez, F. L., & Fernández, R. P. P. (2018). Cómo implantar un SGSI según une-en ISO/IEC 27001 y su aplicación en el esquema nacional de seguridad. Retrieved from https://ebookcentral.proquest.com

de información para generar impacto sobre el mismo o sobre las operaciones de las organizaciones.

Riesgos: Es la probabilidad de que una amenaza se materialice, a partir de las vulnerabilidades que pueden llegar a causar daño o impacto en una organización.

2.2 MARCO TEÓRICO

De acuerdo a la revista UNISCI (2016) – (Unidad de Investigación sobre Seguridad y Cooperación)[8] "El ciberespacio es un escenario de conflicto altamente complejo al estar en constante evolución", donde ninguno de los actores (personas, Hardware, Software) está a salvo de las amenazas provenientes de este entorno, donde no solo afectan las personas sino también la economía y las organizaciones.

Dentro del estudio realizado por UNISCI se destaca los riesgos y amenazas de infraestructuras críticas, donde según los últimos ciberataques ha permitido evidenciar un impacto significativo causando impacto en la continuidad de las operaciones críticas de las organizaciones.

Teniendo en cuenta estos cambios e impactos, las organizaciones y sobre todo los encargados de TI debieron ampliar su visión de seguridad dejando de centrarse solo en la infraestructura tecnológica que tienen en sus datacenters, a tener también en cuenta los aspectos que están relacionados a ellos como son las personas, los servicios publicados en la red, entre otros aspectos que se han ido involucrando en los entornos TIC, generando identificación de riesgos e implementación de controles que mitiguen impactos significativos para la continuación de las operaciones en las Organizaciones[9].

[8] Nieva Machín1 y Manuel Gazapo, la Ciberseguridad como factor crítico en la Seguridad de la unión europea, 2016, Revista UNISCI / UNISCI Journal, Nº 42.

[9] Consultoría para la Implementación de un Marco de Ciberseguridad ISO/IEC 27032, 2018, Internet Security Auditors 2018, https://www.isecauditors.com/consultoria-csf-iso-27032

El ciberespacio es un entorno complejo de actuación entre los diferentes activos de información (personas, Software, internet, entre otros), generando brechas de seguridad para las organizaciones debido a que los servicios brindados en el ciberespacio no son soportados por el mismo proveedor, regulaciones, u otros aspectos que hacen que no se tengan en cuenta las brechas de seguridad entorno a las organizaciones, exponiendo la información sensible.

Teniendo en cuenta estos cambios y la necesidad de cerrar las brechas de seguridad surge la necesidad para que las organizaciones cuenten con políticas, procedimientos, recursos técnicos y humanos necesarios para gestionar efectivamente los riesgos a los cuales están expuestos en el ciberespacio, para lo cual surgió el estándar ISO 27032 el cual hace parte de la familia de normas ISO 27000, aunque esta norma no es certificable si proporciona un marco de buenas prácticas para mejorar el estado de la Ciberseguridad en las organizaciones, tomando en cuenta los diferentes aspectos a los cuales se deben enfrentar cuando publican o trasladan la información sensible o del desarrollo de sus operaciones al ciberespacio, de tal forma que se identifiquen, comprendan, gestionen los riesgos, determinando las actividades más importantes y/o críticas y la entrega de servicios identificando los activos, las personas interesadas, los roles que desempeñan en el ciberespacio de tal forma que se establezcan directrices y/o controles que brinde seguridad en este aspecto a toda la organización.

Al ser parte de la familia de normas 27000 estas buenas prácticas pueden estar incluidas dentro del SGSI, al no solo dar alcance a la implementación de controles para la información, sistemas locales o bajo la administración directa del área de TI sino también a los que están expuestos en el ciberespacio, teniendo en cuenta que estos contienen información sensible o critica de las estrategias de las organizaciones.

2.3 MARCO JURÍDICO

Con los avances tecnológicos, las compañías que cuentan con información de sus operaciones en el Ciberespacio deben contar con estrategias que garanticen la protección de la información en este entorno implementando mejores prácticas que les permita garantizar la seguridad basadas en las leyes y/o regulaciones definidas por el entorno en el cual se encuentra la información algunas de ellas son:

Ley Estatutaria 1266 del 31 de diciembre de 2008 Contiene disposiciones legales del Habeas Data y la regulación de la protección de datos personales**.**

Ley Estatutaria 1581 de Octubre de 2012 por la cual se dictan disposiciones generales para la protección de datos personales, siguiendo la sentencia C-748 de 2011 de la Corte Constitucional y el Congreso de la Republica.

Ley Estatutaria 1273 de enero de 2009 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Circular Externa 007 de Junio de 2018 mediante la cual adicionan el Capítulo V "Requerimientos mínimos para la gestión del riesgo de Ciberseguridad" al Título IV de la Parte I de la Circular Básica Jurídica (C.E. 029 de 2014).

Circular Externa 008 de Junio de 2018 mediante la cual se actualiza el Capítulo I "Canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros" del Título II de la Parte I de la Circular Básica Jurídica (C.E. 029 de 2014).

Resolución AG/RES 2004 (XXXIVO/04) de la Asamblea General de la Organización de los Estados Americanos, la cual establece la Estrategia Integral para combatir las amenazas a la seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética.

GDPR de mayo de 2018, mediante la cual se amplía el alcance de la legislación europea sobre protección de datos, abarcando empresas no europeas que ofrezcan bienes y servicios a residentes en Europa como sucede con varias organizaciones de Colombia.

2.4 ESTADO DEL ARTE

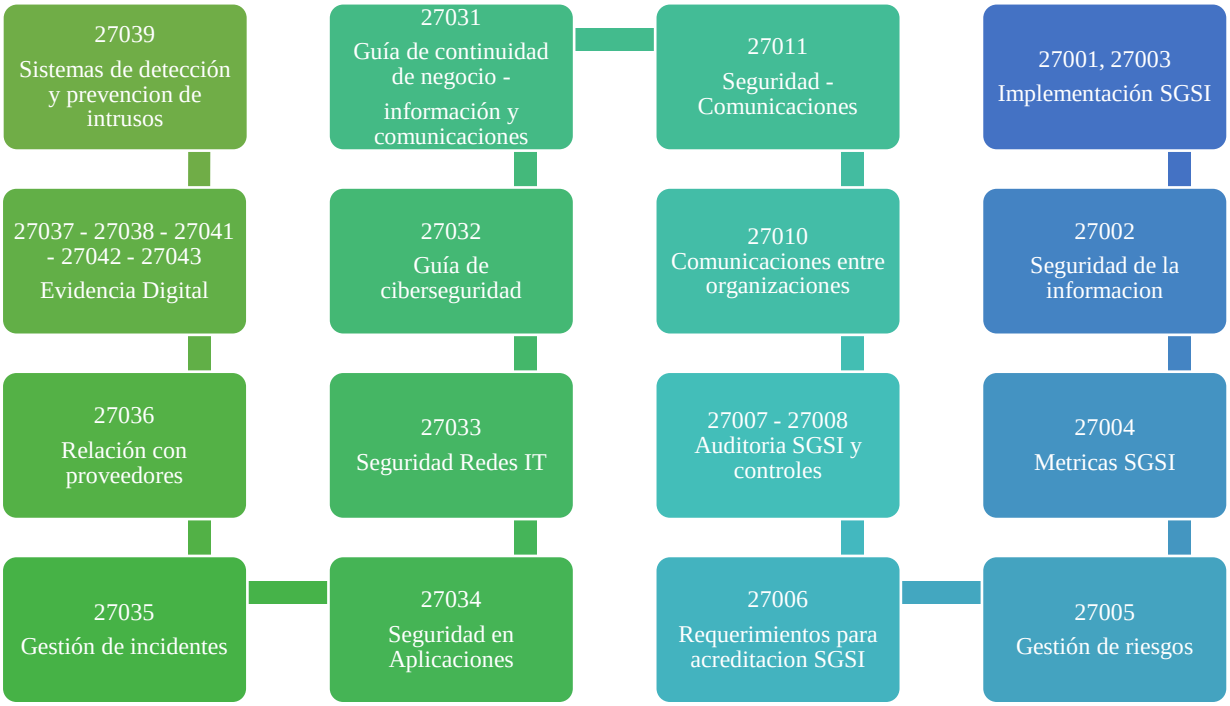
Los avances tecnológicos han permitido automatizar los procesos de las organizaciones permitiendo que estas sean cada día más competitivas en el mercado que se desarrollan, con estos cambios nacieron las buenas prácticas de la ISO 27000 para apoyar el desarrollo de la seguridad de TI, posteriormente crearon un estándar certificable como es la ISO 27001 la cual permite a las organización contar con los lineamientos mínimos para garantizar la integridad, confidencialidad y disponibilidad de la información, pero adicionalmente se han creado otros estándares los cuales apoyan la implementación del SGSI.

Sin embargo con el paso de los años llego un nuevo concepto como es el ciberespacio y muchas de las organizaciones empezaron a migrar su información allí, pero no contaban con controles que les garantizara la seguridad de la misma, por ello nació el estándar ISO 27032 la cual brinda orientación para fortalecer el estado de la Ciberseguridad utilizando los puntos técnicos y estratégicos más importantes que están relacionados con la seguridad en: Redes, internet, información y aplicaciones.

En la figura 4 se observa que el estándar ISO 27000, está conformado por una serie de buenas

prácticas definidas para el aseguramiento de la información en las organizaciones desde diferentes aspectos claves.

Figura 7 – Estructura ISO 27000



Fuente: El Autor

De acuerdo a la figura anterior se puede concluir que los encargados de la seguridad de información, cuentan con diferentes lineamientos que les permite evaluar e implementar controles que mitiguen los riesgos a los cuales se enfrentan en este aspecto.

Según la publicación 8 de los Foros Isis de la Universidad de los Andes (2018)[10], uno de los factores

[10] Ciberseguridad en la era del internet de las cosas, 2018, pág. 11, Universidad de los Andes, https://sistemas.uniandes.edu.co/images/forosisis/revista/8/pdf/FOROS-ISIS-8.pdf. (Andes, 2018)

que se ha vuelto prioridad en las políticas industriales es la seguridad cibernética, de acuerdo al artículo este aspecto aun no hace parte de la cultura organizacional, dado que continúan enfocando sus riesgos en los daños a las maquinas o los accidentes a los empleados, dejando de lado los sistemas de información que cuentan con muchos años en las organizaciones y en algunas de ellas como no han presentado fallas no cuentan con antivirus y/o parches necesarios para mitigar incidentes de seguridad en los cuales se vea comprometida la información. La ausencia de la cultura de seguridad y la carencia de monitoreo continuo, genera que las organizaciones no estén preparadas para la respuesta a incidentes de Ciberseguridad, dado que en muchas ocasiones no cuentan con áreas o expertos de Seguridad de TI que se encarguen de monitorear periódicamente estos aspectos de la infraestructura tecnológica, implementando buenas prácticas que les permita estar preparadas de una manera más óptima para dar respuesta a los incidentes.

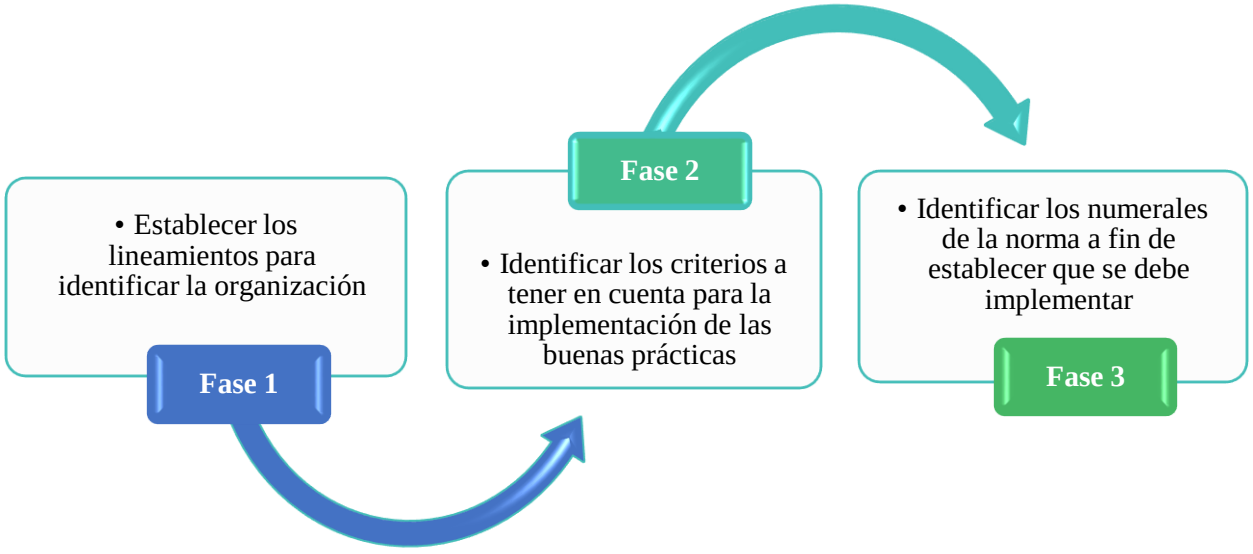
Dentro del artículo presentado en los foros de la Universidad de los Andes se observan diferentes situaciones que se han presentado en organizaciones a nivel mundial los cuales se han generado desde fuentes como correos Spearphishing, Watering Hole, entre otros. Adicionalmente el conferencista enumera algunos puntos a ser tenidos en cuenta a la hora de evaluar la seguridad de las organizaciones empezando por mejorar lo que se tiene como dispositivos y personas seguras, uso de protocolos estándar, auditar todos los accesos, usar autenticación de dos factores, entre otros antes de implementar nuevas mejoras.

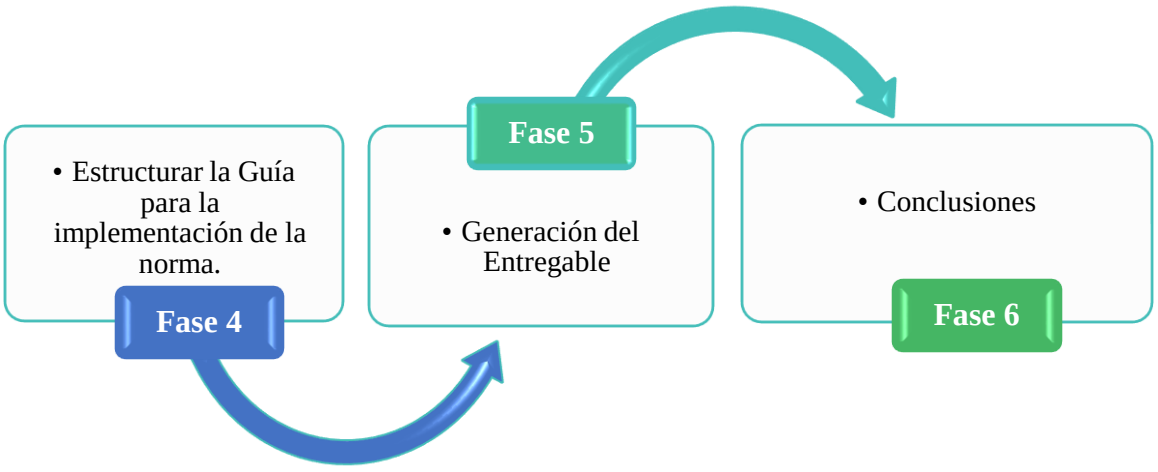
3 METODOLOGÍA

El enfoque de esta investigación es de carácter cuantitativo dado que se pretende realizar una recolección de información mediante marcos de referencia como lo es COBIT, la cual permitirá identificar cada uno de los requerimientos y/o lineamentos definidos por la norma ISO 27032 para ser aplicada en las organizaciones.

3.1 FASES DEL TRABAJO DE GRADO

Figura 8 – Fases del Trabajo de Grado





Fuente: El Autor

Fase 1:

Establecer los lineamientos para identificar la organización: Definir un formato en el cual se pueda identificar el sector al cual está asociada, el tipo o modelo de negocio, la regulación bajo la cual se debe regir, los productos o servicios que brinda, el tipo de tecnología implementada, los mecanismos de seguridad con los que cuenta, entre otros.

Fase 2:

Definir los criterios a tener en cuenta para la implementación de las buenas prácticas: de la ISO 27032 en las organizaciones, a fin de establecer el alcance, de la implementación, recursos y otros.

Fase 3:

Identificar los numerales de la norma a fin de establecer que se debe implementar: Evaluar cada uno de los numerales y establecer cuales son de información general y cuáles son los lineamientos y/o buenas prácticas a implementar.

Fase 4:

Estructurar la Guía para la implementación de la norma: Definir los lineamientos y estructura

para cada uno de los ítems identificados en la norma, tomando como base el PH (Planear y Hacer) de la metodología PHVA o ciclo de Deming la cual está basada en un concepto ideado por Walter Shewhart, esta metodología es muy utilizada para la implementación de los diferentes sistemas de información asociados a las normas ISO como la 9001 – Calidad, 27001 – Seguridad de la Información entre otros. Esta se divide en cuatro pasos que se definen de la siguiente manera:

Planear: Establecer los objetivos y procesos necesarios para conseguir los resultados, en este paso se debe tener en cuenta los siguiente, el que, como y para que se planeó.

Hacer: definir los entregables para cada uno de los numerales, teniendo en cuenta la información recolectada para la organización identificando quien, cuando y como se ejecuta el proceso.

Verificar: Realizar seguimiento y medición a lo implementado para cada uno de los procesos a fin de establecer si es acorde o no para las actividades que desarrollan o si requieren mejoras para que sean óptimos.

Actuar: Tomar acciones para mejorar continua, de acuerdo a lo identificado en el verificar y generar los cambios que garanticen la efectividad y eficiencia en el proceso.

Fase 5:

Generación del Entregable: Generar el entregable en el cual las organizaciones se podrán apoyar para la implementación de las buenas prácticas definidas en la Norma ISO 27032.

Fase 6:

Conclusiones: De acuerdo a los comentarios y resultados del entregable concluir la investigación y generar las recomendaciones a tener en cuenta para el momento de la aplicación de este documento.

3.2 ALCANCES Y LIMITACIONES

Crear una guía para la implementación de controles de Ciberseguridad en las organizaciones, tomando como base la norma ISO 27032 mediante la cual se pueda identificar cada uno de los factores que define la misma a fin de establecer las mejores prácticas que les permita estar preparadas para dar respuesta de manera efectiva a un incidente en el cual se vean comprometidos los activos que están en el ciberespacio y que pueden llegar a ser críticos para la continuidad de sus operaciones. Partiendo de la premisa que cada organización está expuesta a riesgos diferentes a pesar de enfocarse o pertenecer al mismo sector o mercado.

Dentro de las limitaciones del proyecto está la ausencia y/o desinterés por parte de la Alta Gerencia para la implementación de las buenas prácticas definidas en la ISO 27032, así como la falta de personal capacitado o con conocimiento pleno de la organización y su infraestructura tecnológica la cual es base principal para la adecuada identificación de los riesgos a los cuales están expuestos en el ciberespacio así como la definición de controles que mitiguen el impacto de un incidente cibernético en las operaciones.

3.3 CRONOGRAMA

Tabla 1 – Detalle del Cronograma

Nombre de tarea	Duración	Costo	% completado	Nombres de los recursos	Comienzo	Fin
Guía Para Implementar la norma ISO 27032	**170,88 días**	**$6.764000**	**100%**	**Computador[2], Internet[1], Resma de papel[1 Resma]**	**lun 10/09/18**	**lun 06/05/19**
Generalización del Tema	**15 días**	**$1.080.000**	**100%**		**lun 10/09/18**	**vie 28/09/18**
Identificación de necesidades	80 horas	$720.000	100%	Persona 1	lun 10/09/18	vie 21/09/18
Selección del Tema	40 horas	$360.000	100%	Persona 1	lun 24/09/18	vie 28/09/18
Planteamiento del Problema	**17,5 días**	**$1.524.000**	**100%**		**lun 01/10/18**	**mié 24/10/18**
Antecedentes del problema	26 horas	$234.000	100%	Persona 1	lun 01/10/18	jue 04/10/18
Formulación Pregunta de Investigación	26 horas	$156.000	100%	Asistente	lun 01/10/18	jue 04/10/18
Justificación	26 horas	$234.000	100%	Persona 1	lun 01/10/18	jue 04/10/18
Objetivos: General y Específicos	50 horas	$300.000	100%	Asistente	jue 04/10/18	mié 17/10/18
Marco Conceptual	20 horas	$120.000	100%	Asistente	lun 22/10/18	mié 24/10/18
Marco Teórico	20 horas	$180.000	100%	Persona 1	lun 22/10/18	mié 24/10/18
Marco Jurídico	20 horas	$120.000	100%	Asistente	lun 22/10/18	mié 24/10/18
Estado del arte	20 horas	$180.000	100%	Persona 1	lun 22/10/18	mié 24/10/18
Metodología	**15 días**	**$1.080.000**	**100%**		**lun 05/11/18**	**vie 23/11/18**
Definición de la Metodología	16 horas	$144.000	100%	Persona 1	lun 05/11/18	mar 06/11/18
Determinar las fases del Trabajo de Grado	16 horas	$144.000	100%	Persona 1	mié 07/11/18	jue 08/11/18
Definición productos a entregar	16 horas	$144.000	100%	Persona 1	vie 09/11/18	lun 12/11/18
Cronograma	16 horas	$144.000	100%	Persona 1	mar 13/11/18	mié 14/11/18
Presupuesto	16 horas	$144.000	100%	Persona 1	jue 15/11/18	vie 16/11/18
Generar el Documento y Presentación	40 horas	$360.000	100%	Persona 1	lun 19/11/18	vie 23/11/18

Desarrollo del proyecto	**50,88 días**	**$2.874.000**	**100%**		**lun 04/03/19**	**lun 13/05/19**
Ajustar documento	39 horas	$234.000	100%	Asistente	lun 04/03/19	vie 08/03/19
Establecer los lineamientos para identificar la organización	40 horas	$240.000	100%	Asistente	vie 08/03/19	vie 15/03/19
Identificar los criterios a tener en cuenta para la implementación de las buenas practicas	80 horas	$720.000	100%	Persona 1	vie 15/03/19	vie 29/03/19
Identificar los requisitos para cada uno de los numerales	80 horas	$480.000	100%	Asistente	lun 01/04/19	lun 15/04/19
Estructurar la guía para la evaluación de la norma	40 horas	$360.000	100%	Persona 1	lun 15/04/19	lun 22/04/19
Generación del Entregable	80 horas	$480.000	100%	Asistente	lun 22/04/19	lun 06/05/19
Conclusiones	40 horas	$360.000	100%	Persona 1	lun 06/05/19	lun 13/05/19
Documento Final	0 horas	$0	100%	Persona 1	lun 13/05/19	lun 13/05/19

Fuente: El Autor

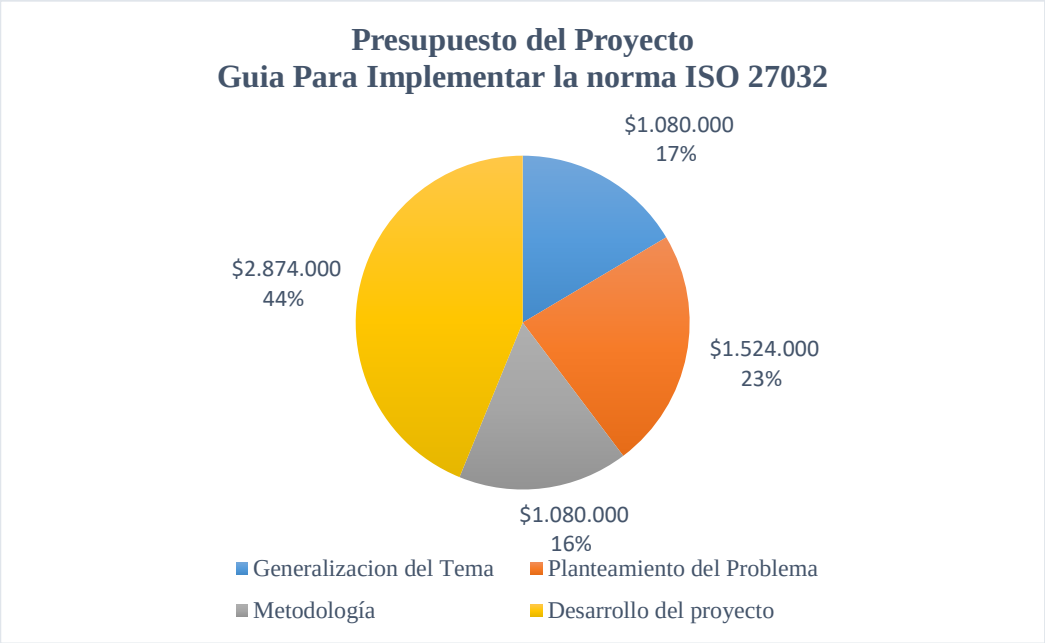
3.4 PRESUPUESTO

Tabla 2 – Presupuesto Proyecto

Nombre	Costo Por Tarea	Costo Total
Generalización del Tema		**$ 1.080.000**
Identificación de necesidades	$ 720.000	
Selección del Tema	$ 360.000	
Planteamiento del Problema		**$ 1.524.000**
Antecedentes del problema	$ 234.000	
Formulación Pregunta de Investigación	$ 156.000	
Justificación	$ 234.000	
Objetivos: General y Específicos	$ 300.000	
Marco Conceptual	$ 120.000	
Marco Teórico	$ 180.000	
Marco Jurídico	$ 120.000	
Estado del arte	$ 180.000	
Metodología		**$ 1.080.000**
Definición de la Metodología	$ 144.000	
Determinar las fases del Trabajo de Grado	$ 144.000	
Definición productos a entregar	$ 144.000	
Cronograma	$ 144.000	
Presupuesto	$ 144.000	
Generar el Documento y Presentación	$ 360.000	
Desarrollo del proyecto		**$ 2.874.000**
Ajustar documento	$ 234.000	
Establecer los lineamientos para identificar la organización	$ 240.000	
Identificar los criterios a tener en cuenta para la implementación de las buenas practicas	$ 720.000	
Identificar los requisitos para cada uno de los numerales y tipo de sector al que aplica	$ 480.000	
Estructurar la guía para la evaluación de la norma	$ 360.000	
Generación del Entregable	$ 480.000	
Conclusiones y Recomendaciones	$ 360.000	
Documento Final	$ -	
Computar y Resma de papel	$ -	$ 206.000
Guía Para Implementar la norma ISO 27032		**$ 6.764.000**

Fuente: El Autor

Figura 9 – Distribución del presupuesto



Fuente: El Autor

4 PRODUCTOS A ENTREGAR

Con la identificación de las necesidades y el problema a resolver a lo largo de la investigación, se define como producto a entregar una guía que le permita a las organizaciones implementar de manera eficiente cada uno de los ítems que contiene la norma ISO 27032, de acuerdo al sector o mercado al cual pertenecen, estableciendo controles que les permita estar preparados para dar respuesta de manera eficiente a los incidentes de Ciberseguridad de los cuales pueden ser víctimas al tener información crítica e importante publicada en la red o en entornos virtuales que no son administrados de manera efectiva o están tercerizados.

Para ello a continuación se relacionan los entregables definidos de acuerdo a los objetivos propuestos en esta investigación, a fin de garantizar el alcance de los mismos.

Tabla 3 – Entregables definidos

Objetivo	Entregable
Identificar las buenas prácticas de Ciberseguridad en las organizaciones de acuerdo a los requerimientos establecidos en la norma ISO27032.	a. Plantilla para realizar el Entendimiento de la organización, identificando: ✓ Misión ✓ Objetivo del Negocio. ✓ Tipo de organización ✓ Tamaño de la organización ✓ Sistemas de Gestión Implementados. ✓ Listado de procesos. ✓ Sistemas de información. ✓ Tipo de infraestructura (Física, Nubes, propia, tercerizada)

Objetivo	Entregable
	✓ Mecanismos de Seguridad Implementados. ✓ Activos con los que cuenta la organización ✓ Análisis de riesgos ✓ Evaluación de Vulnerabilidades b. Modelo Evaluación de diagnóstico de Seguridad, mediante una herramienta libre.
Definir criterios para evaluar la implementación de las buenas prácticas de Ciberseguridad en las organizaciones de acuerdo a la norma ISO 27032.	Generar la lista de los criterios a tener en cuenta para la implementación y de acuerdo a los resultados obtenidos en el diagnóstico, establecer sobre cuales se deben enfocar con más atención.
Establecer los lineamientos para implementar los controles y hacer seguimiento a la implementación de las buenas prácticas de Ciberseguridad de acuerdo a la norma ISO 27032	Definir la guía para la implementación y evaluación de la ISO27032 en cualquier compañía, la cual debe contener: a. Establecer los objetivos para cada numeral. b. Definir el ciclo PHVA para cada numeral. c. Identificar las normas, circulares u otros (CE007/2018 - SFC, ISO 27001) en los cuales se puedan apoyar para la implementación.

Fuente: El Autor

5 ENTREGA DE RESULTADOS ESPERADOS E IMPACTOS

5.1 METODOLOGÍA PROPUESTA

5.1.1 CONTEXTUALIZACIÓN DE LA NORMA

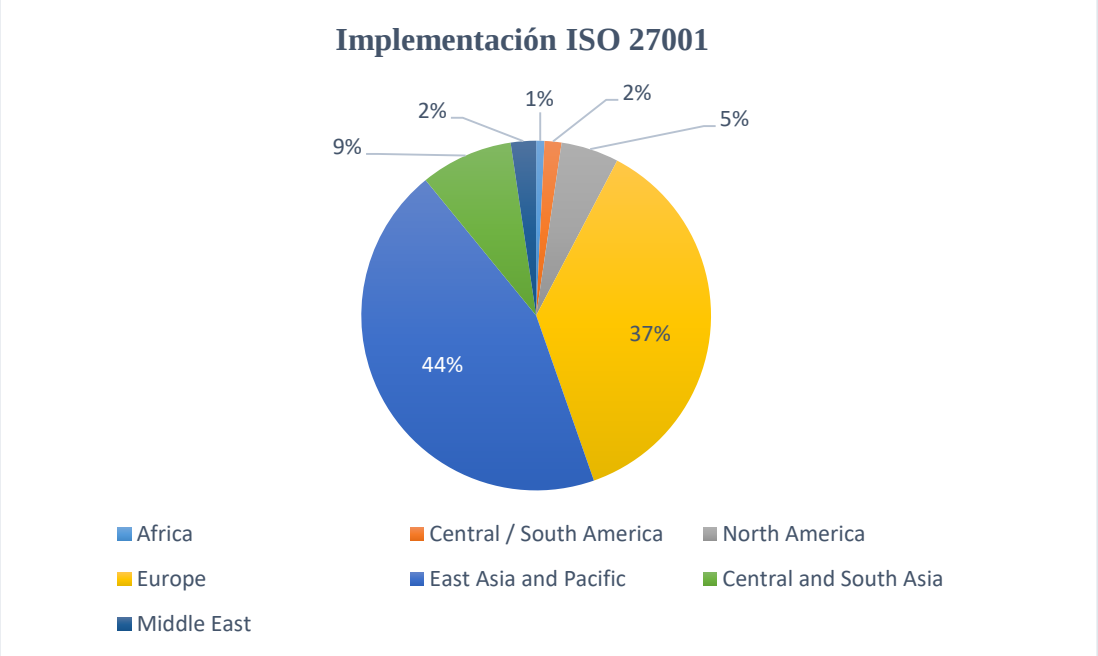
Las organizaciones tienen la visión que un sistema de gestión solo se puede implantar en grandes compañías, dado que requieren recursos físicos y lógicos los cuales por su tamaño no son posibles adquirir debido a que esto generaría una inversión representativa, para la cual no tienen recursos destinados, adicional a ello, los beneficios se ven reflejados más en compañías pequeñas que grandes, debido a que las primeras al estar iniciando pueden ir adoptando buenas prácticas mediante controles que les permita mitigar riesgos, que podrían llegar a ser más complejos de controlar en las grandes compañías por su tamaño, estructura y/o cultura digital.

Muchas de las organizaciones han iniciado por implementar sistemas de gestión de calidad, los cuales están enfocados en estructurar sus procesos y generar procedimientos que optimicen y controlen de manera efectiva sus operaciones y/o actividades, sin embargo con los avances tecnológicos y a fin poder competir en el mercado adquieren tecnología de última generación y es allí donde surge la necesidad de establecer controles que mitiguen los riesgos a los que se ven expuestos. A nivel de TI uno de los estándares más utilizados por las compañías es la ISO 27001, sin embargo de acuerdo a la encuesta anual de la ISO[11] en Colombia son pocas las compañías que se han certificado en este estándar. A Continuación se detallan los resultados a nivel mundial, por continente y país, donde se observa que a 2017 a nivel mundial existían 39.501 certificados de ISO 27001 de los cuales solo el 1,6% corresponde a América Central y Latinoamérica, ubicando a

[11] The ISO Survey, 2018, International Organization for Standardization, https://www.iso.org/the-iso-survey.html. (ISO, ISO Survey, 2018)

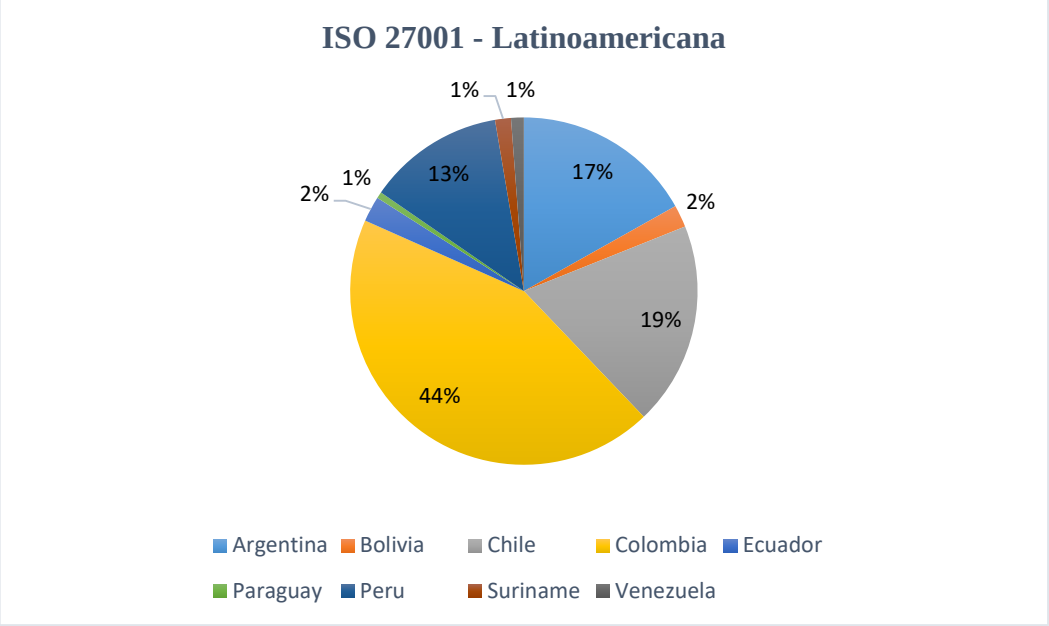
Colombia es el segundo país con más certificados, adicionalmente la encuesta refleja que existían 148 certificados, lo que nos indica que en el país a pesar de tenerlas como referentes para cumplimientos legales y en otros casos ser usadas como mejores prácticas, o mencionadas en sus políticas y manuales, no están adoptadas en su totalidad. Esto se puede asociar a factores como la falta de expertos y/o conocimientos dentro de la organización para implementar un estándar sin tener en cuenta que estos proporcionan una base sólida que puede aplicarse en el desarrollo de las regulaciones nacionales e internacionales, como sucede con el sector Financiero en Colombia donde son tomadas como referencia pero prima las regulaciones de la Superintendencia Financiera. Estos resultados se pueden observar en las figuras 10 y 11 que se presentan a continuación.

Figura 10 - Resultados Encuesta 2017 – ISO



Fuente: SO Survey 2017 – Resultados Mundiales,
https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

Figura 11 – Implementación ISO 27001 en Latinoamérica



Fuente: SO Survey 2017 – Resultados Mundiales,
https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

Las figuras anteriores nos dan una visión a nivel general de la implementación de la ISO27001 a nivel global, donde claramente se puede concluir que para las organizaciones no es una prioridad estar certificados en este estándar.

Luego de los resultados de la ISO, nos enfocaremos en la ISO 27032 la cual nace como un complemento a la ISO27001, cuyo fin es brindar las mejores prácticas para la protección de los activos virtuales (Sistemas e Información), críticos, entre otros, los cuales son parte fundamental para el desarrollo de sus operaciones. Donde de acuerdo a lo investigado las organizaciones no conocen como adaptar o certificarse en estándares como los de la familia ISO27000. Para ello a continuación se detallan las pautas a tener en cuenta para implementar estas buenas prácticas.

5.1.2 ENTENDIMIENTO DE LA ORGANIZACIÓN

Inicialmente se debe realizar una identificación de la Organización para la cual se implementara: en este ítem se generara el entendimiento, que permitirá conocer el tipo de compañía, objetivos del negocio, misión, sistemas de gestión implementados como ISO27001, ISO9001, aspectos regulatorios, infraestructura tecnología, entre otros elementos que permitan no solo conocer la organización sino establecer qué tan preparados están frente a la Ciberseguridad. Para ello se debe tener en cuenta lo siguiente:

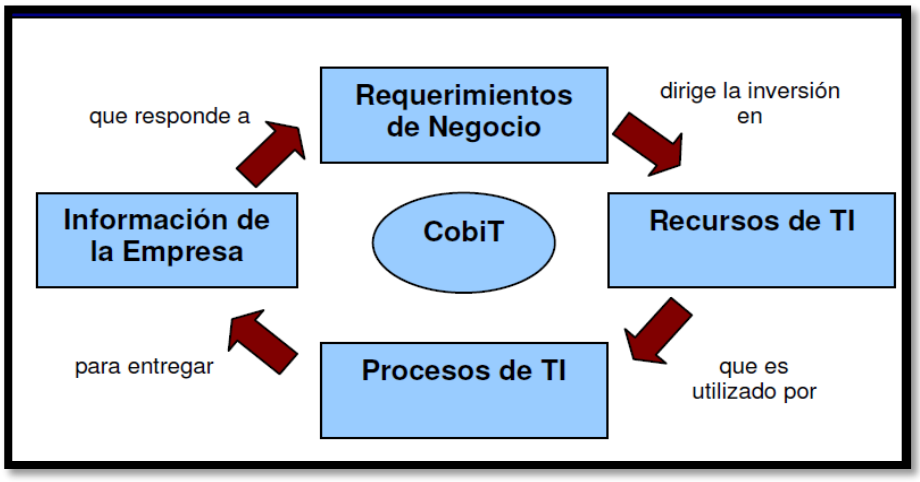
- ✓ Establecer si se debe aplicar o no la norma ISO27032: en este aspecto se definirán criterios que permitan identificar que ítems deberían de implementar en su totalidad, o cuales aspectos requieren fortalecer de acuerdo a lo que tienen actualmente implementado, y a las buenas prácticas definidas en la norma.
- ✓ Definir para cada uno de los numerales de la norma, los lineamientos a tener en cuenta para la implementación de estas buenas prácticas, en la organización y que se requeriría para la implementación.

Para el desarrollo de esta guía iniciaremos por un diagnóstico, el cual se identificaran cada uno de los activos de información junto con su criticidad, así como el nivel de exposición al riesgo respecto a su nivel de preparación, donde para este segundo aspecto se tomara como referencia una aplicación Free que esta publicada en las market de los sistemas operativos móviles y puede ser ejecuta en cualquier organización y/o sector.

Basados en las buenas prácticas de COBIT, se creó una plantilla mediante la cual se podrá realizar un entendimiento de la organización de tal manera que se establezca quienes la componen, cuál es su infraestructura, cuáles son sus niveles de seguridad, entre otros aspectos que son

requeridos obtener una visión general de la misma. En la siguiente gráfica se observan los criterios o lineamientos de COBIT que se tomaron como referencia para la creación de la plantilla.

Figura 12 – Principios Básicos de COBIT



Fuente: COBIT 4.1

Como se observa en la Figura 12, se debe tener en cuenta el ciclo donde se determine y/o identifiquen los requerimientos del negocio, los recursos y procesos de TI que permitirán entregar la información al negocio para la ejecución de sus procesos.

De acuerdo a lo anterior a continuación se detalla la plantilla que se creó para realizar un entendimiento a nivel general de la organización, donde se podrá conocer la misión, visión, objetivos, identificar su infraestructura, sistemas, criticidad de los mismos, proyectos, administración de la infraestructura, entre otros aspectos generales de TI, que serán base para la implementación de la norma ISO27032.

Tabla 4 – Conocimiento de la Compañía

Conocimiento de la Compañía	
Objetivo: Conocer la compañía a fin de establecer su tamaño, tipo de organización, tipo de tecnologías, entre otros aspectos que permitirán determinar la mejor ruta para la implementación de las buenas prácticas dela ISO 27032	
Información General	
Nombre	
Sector	
Tipo de organización	
Objetivo del negocio	
Misión	
Visión	
Cantidad de Procesos	
# empleados	
Información Alta Dirección	
Involucran a la alta dirección está en los temas de seguridad	
Cuentan con el apoyo de la alta dirección para la implementación de mecanismos de Seguridad	
La Alta Dirección es capacitada en temas de Seguridad	
Presentan periódicamente a la Alta Dirección el estado de la seguridad de la compañía indicando incidentes, planes de acción, entre otros.	
Estructura de TI y Seguridad	
Conocer como está definida la estructura de compañía a nivel de TI y seguridad	

Conocimiento de la Compañía	
Que áreas existen en TI	
Cuenta con especialistas de Seguridad de la información e informática	
Existe un oficial de Seguridad	
Cuentan con área de Riesgos – Que procesos tienen allí.	

Descripción Tecnología	
Conocer los sistemas y servicios con los que cuenta la organización.	
Ítem	**Descripción**
Que sistemas tiene	
Cuantos son propios	
Cuantos son tercerizados	
Cuantos son por suscripción	

Seguridad informática y de la información.	
Conocer los mecanismos de seguridad con los que cuenta la organización.	
Ítem	**Descripción**
Hardware	
Software	
Cuentan con mecanismos de cifrado para la transferencia de información.	
Existen mecanismos de seguridad para el acceso a internet a fin de mitigar huecos de seguridad.	

Conocimiento de la Compañía	
Para cada uno de los sistemas y servicio identificados, establecer los mecanismos de seguridad.	
Controles lógicos	
Cuentan con roles y perfiles para el acceso a los sistemas	
Cuál es el proceso para asignar usuarios y roles.	
Los cambios a los sistemas cuentan con un procedimiento para su implementación.	
En caso de tener Software tercerizado, cuentan con un procedimiento para estos cambios.	
Cuentan con políticas de acceso para los sistemas de información cuando están conectados a una red diferente a la corporativa.	
Que mecanismos tienen definidos para el acceso de los terceros a los sistemas de información.	

Detalle Jurídico /cumplimiento	
Conocer el entorno regulatorio en el cual se desenvuelve la compañía a fin de identificar que regulación se debe tener en cuenta para implementar las buenas prácticas de Ciberseguridad.	
Ítem	**Descripción**
Circulares	
Decretos	

Conocimiento de la Compañía	
Leyes	
Sistemas de Gestión Implementados	
Que sistemas de Gestión tienen implementados y en qué % se encuentran certificados.	
ISO9001	
ISO27001	
Otro	
Que sistemas de Gestión tienen implementados y en qué % se encuentran certificados.	
Que Políticas tiene Implementadas a nivel de seguridad y Ciberseguridad	
Manejo de incidentes	
Tiene implementado un SOC	
Cuenta con una base de Incidentes	
Tiene establecida una Política de manejo de incidentes de Seguridad	
Concientización y Capacitación	
Tienen un cronograma de capacitación respecto a Ciberseguridad	

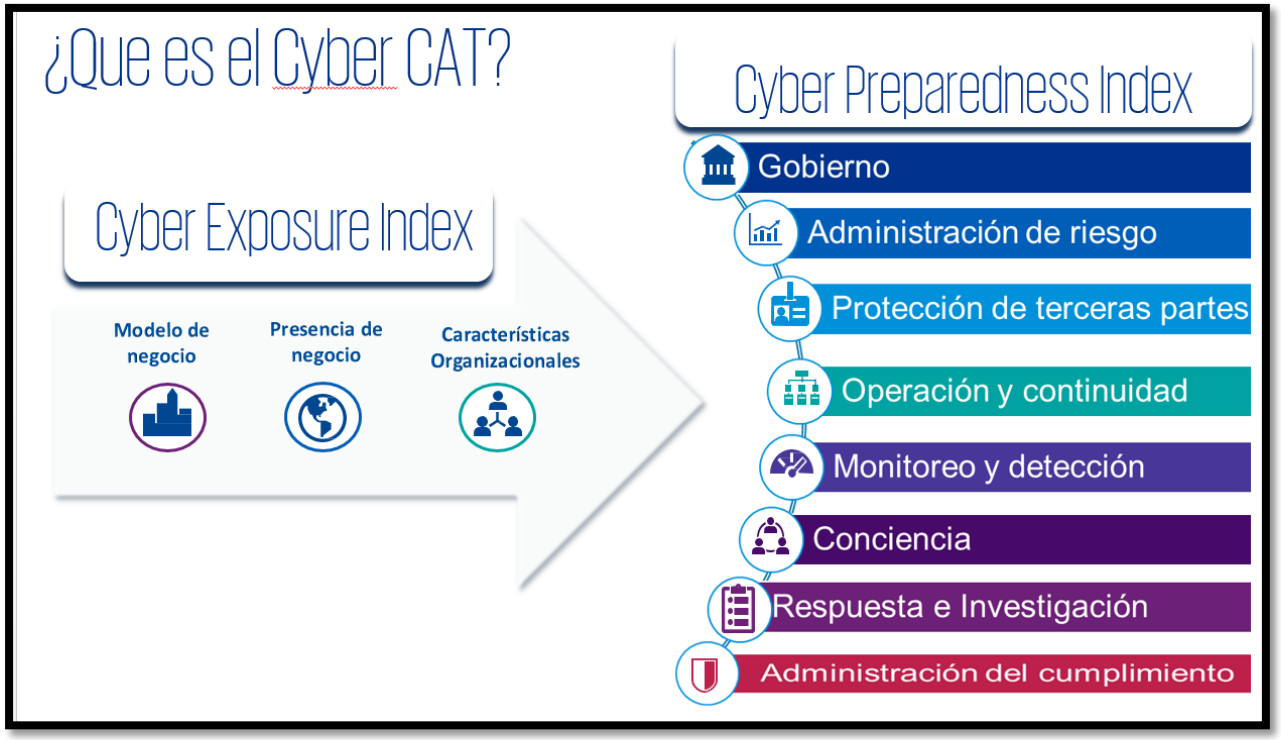
Conocimiento de la Compañía	
Realizan campañas periódicas de concientización sobre ataques cibernéticos.	
Realizan algún seguimiento a los temas de concientización y/o capacitación.	

Fuente: El Autor

Luego de conocer la organización mediante la plantilla definida en la Tabla 4, se requiere establecer e identificar el nivel de exposición y preparación de la organización, para ello se utilizara una herramienta free que permite realizar el diagnostico en estos aspectos, la cual se llama Cyber CAT, esta es una aplicación móvil, desarrollada por KPMG una de las 4 Big Four de consultoría, la cual mediante unas preguntas les permite realizar una autoevaluación de su postura de seguridad cibernética de manera repetible y mensurable, enfocándose en dos aspectos, el primero es la exposición al riesgo, y el segundo es la preparación de la organización para responder a incidentes, evaluando elementos como el gobierno, gestión del riesgo cibernético y la respuesta a investigación de incidentes, que permite contar con lecciones aprendidas para mitigar impactos en sus procesos críticos.

A Continuación se detallan los componentes de la herramienta:

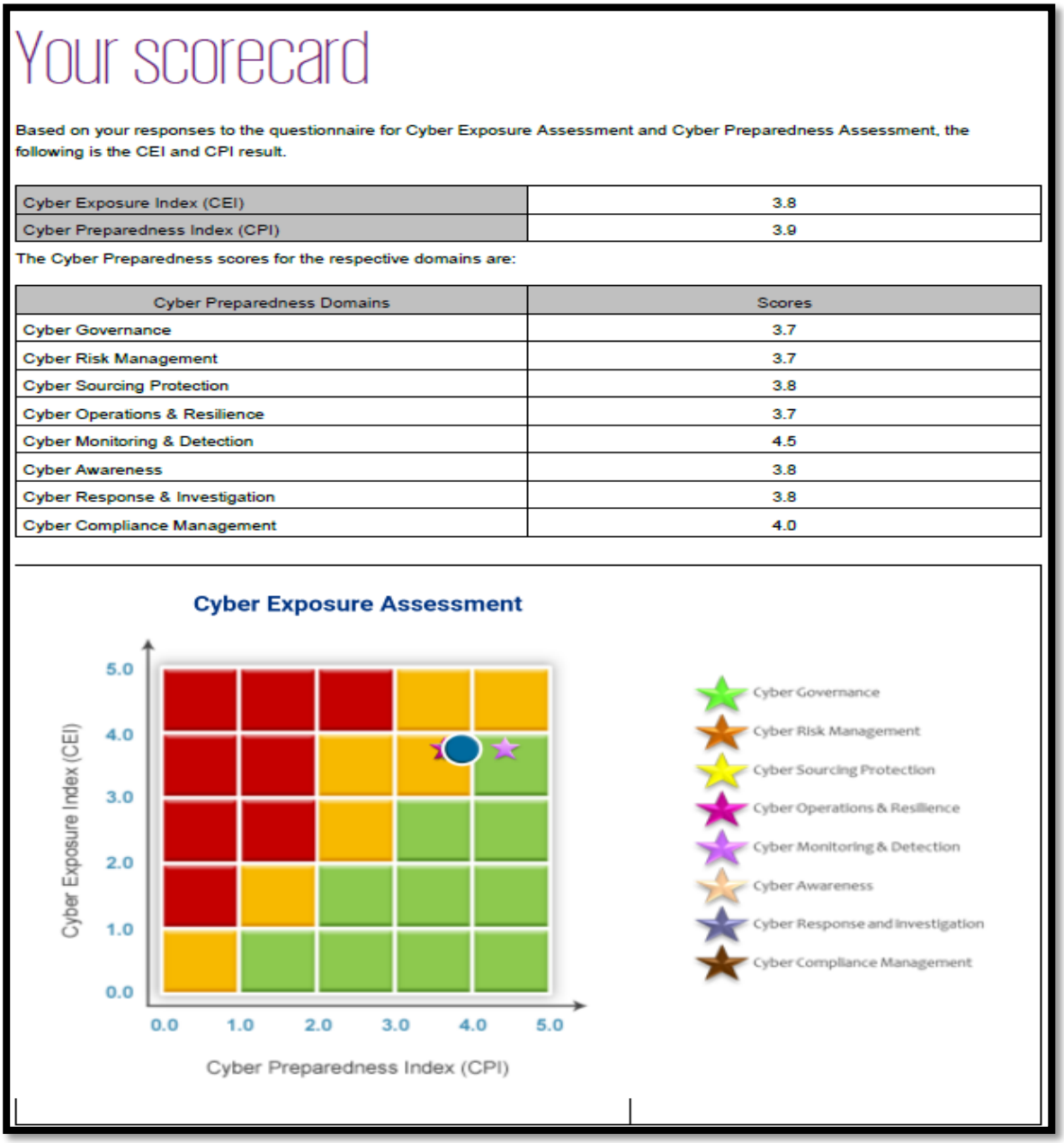
Figura 13 – Estructura Cyber CAT



Fuente: KPMG Colombia.

Mediante una calificación que para cada uno de los ítems evaluados y una gráfica permite visualizar el estado de la organización, los criterios en los cuales se debe enfocar con más precisión, es posible identificar los puntos donde requieren implementar controles que les permita mitigar los riesgos de Ciberseguridad.

Figura 14 - Ejemplo Resultados del Diagnostico



Your scorecard

Based on your responses to the questionnaire for Cyber Exposure Assessment and Cyber Preparedness Assessment, the following is the CEI and CPI result.

Cyber Exposure Index (CEI)	3.8
Cyber Preparedness Index (CPI)	3.9

The Cyber Preparedness scores for the respective domains are:

Cyber Preparedness Domains	Scores
Cyber Governance	3.7
Cyber Risk Management	3.7
Cyber Sourcing Protection	3.8
Cyber Operations & Resilience	3.7
Cyber Monitoring & Detection	4.5
Cyber Awareness	3.8
Cyber Response & Investigation	3.8
Cyber Compliance Management	4.0

Fuente: Herramienta Cyber CAT - KPMG

En la figura anterior se observa el resultado que genera la herramienta, tanto global como por cada ítem y el mapa de calor en el cual se puede observar en qué punto está la organización respecto a los dos componentes evaluados.

5.1.3 CRITERIOS A TENER EN CUENTA

Teniendo en cuenta los elementos y resultados identificados en el entendimiento, se toman como criterios para la implementación de la guía, los siguientes aspectos:

- ✓ Gobierno
- ✓ Administración de Riesgo
- ✓ Protección de terceras partes
- ✓ Operación y Continuidad.
- ✓ Monitoreo y Detección
- ✓ Conciencia
- ✓ Respuesta e Investigación
- ✓ Administración del Cumplimiento.

Los criterios mencionados anteriormente, permiten enfocar la implementación de la norma en aspectos base e importantes para cualquier organización sin importar el tipo de negocio.

5.1.4 GUÍA PARA LA IMPLEMENTACIÓN DE LA ISO 27032

Teniendo en cuenta que la ISO 27032, presenta las buenas prácticas de Ciberseguridad, permite que las mismas se puedan implementar en cualquier compañía, dado que su objetivo es generar lineamientos para la protección de los activos de información que se encuentran en el ciberespacio.

De acuerdo a lo anterior y con el resultado del diagnóstico que se genera mediante la herramienta así como el entendimiento, mencionado en el numeral 5.1.2, la organización podrá conocer e identificar los puntos claves en los cuales está más débil, de tal forma que puedan fortalecerlos con las buenas prácticas de la ISO27032, mediante la implementación de controles

en aspectos como seguridad de información, seguridad de la red, seguridad de Internet y protección de infraestructuras críticas de información, los cuales presenta la norma en 13 numerales, que se mencionan a continuación:

Tabla 5 – Numerales ISO 27032

Numeral	Descripción
1.	Alcance
2.	Aplicabilidad
3.	Referencias
4.	Términos
5.	Abreviaturas
6.	Generalidades
7.	Partes interesadas en el Ciberespacio
8.	Activos en el Ciberespacio
9.	Amenazas contra la seguridad del ciberespacio
10.	Roles de las partes interesadas en la Ciberseguridad.
11.	Directrices para los interesados
12.	Controles de Ciberseguridad
13.	Marco del intercambio de información y la coordinación

Fuente: Norma ISO 27032

En la tabla No. 5 se observan los numerales generales de la norma, con base en los cuales se realizará la guía para la implementación de las buenas prácticas que se presenta allí.

Inicialmente para la implementación de esta norma, se debe contar con:

a. El apoyo de la alta dirección de tal forma que esto garantice la efectividad de la implementación.
b. Persona que conozca de seguridad de la información y Ciberseguridad.
c. Contar con un grupo interdisciplinario de la organización, los cuales conozcan tanto del tema de Tecnología, como de los procesos y un experto en riesgos que apoye el proceso de

evaluación de los mismos para cada uno de los activos.

d. Políticas y procedimientos de la organización en los cuales se puede conocer cada uno de los procesos, junto con sus actividades y activos involucrados para el desarrollo de los mismos.

Con estos elementos principales se debe iniciar con la validación de cada uno de los numerales, para los cuales a continuación se indican los lineamientos, donde se tomara literalmente el campo requerimiento/descripción que se muestra a continuación en cada una de las tablas[12], respecto a los numerales 1-6 no se requiere implementación dado que son de conocimientos de la norma, pero si deben ser consultados dado que permitirán contextualizar a los líderes de Ciberseguridad sobre la norma.

Numeral 1 - Alcance	
Descripción	Esta norma nacional proporciona una guía para mejorar el estado de la Ciberseguridad, destacando aspectos únicos de dicha actividad y su dependencia de otros ámbitos de seguridad, en particular: ✓ Seguridad de la información, ✓ Seguridad de las redes, ✓ Seguridad de internet, ✓ Protección de la infraestructura crítica de información (CIIP). Se cubre el punto partida en prácticas de seguridad para las partes interesadas del Ciberespacio.
Numeral 2 – Aplicabilidad	
Descripción	Audiencia: Proveedores de servicios en el Ciberespacio, consumidores que utilizan estos servicios. Limitaciones: Esta norma nacional no incluye: ❖ La ciberprotección, ❖ El delito informático (cibercrimen),

[12] ISO (ISO, Information technology — Security techniques — Guidelines for cybersecurity, 2012)

	❖ La protección de la infraestructura crítica de información (CIIP), ❖ La seguridad en internet, y ❖ Los delitos relacionados con internet.
Numeral 3 – Referencias Normativas	
Descripción	Como documento de referencia la norma indica la ISO/IEC 27000, Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Descripción general y vocabulario.
Numeral 4 – Términos y Definiciones	
Descripción	La norma toma los términos y definiciones indicados en la ISO/IEC 27000.
Numeral 5 - Abreviaturas	
Descripción	En este numeral se describen las abreviaturas que se usan en los diferentes requerimientos que contiene la norma.
Numeral 6 - Generalidades	
Descripción	La seguridad en Internet y en el Ciberespacio ha sido un tema de creciente preocupación. Las partes interesadas han venido estableciendo su presencia en el Ciberespacio a través de sitios web y ahora están tratando de aprovechar aún más el mundo virtual proporcionado por el Ciberespacio[11]. Dentro de este numeral se describe la naturaleza del Ciberespacio, Ciberseguridad, el modelo general que será tomado como base para el desarrollo de la norma, enfoque el cual está enmarcado en la estrategia para cada una de las partes interesadas.

De acuerdo a lo anterior la guía se enfocará en la implementación en los numerales del 7 al 13, para los cuales la norma presenta los requerimientos o lineamientos que se deben tener en cuenta para la adoptar la buena práctica que se plantea, teniendo en cuenta que no hace diferencia entre organización, actividad o tamaño.

<table>
<tr><th colspan="2">Numeral 7 - Partes interesadas en el Ciberespacio</th></tr>
<tr><td>Objetivos</td><td>Identificar quienes son las partes interesadas dentro de la organización.</td></tr>
<tr><td>Requerimiento</td><td>A los efectos de esta norma, los interesados en el ciberespacio se clasifican
en los siguientes grupos:
• Los consumidores, incluyendo personas y Organizaciones tanto públicas como privadas;
• Proveedores, incluyendo Proveedores de servicios de Internet; y Los proveedores de servicios de aplicaciones.</td></tr>
<tr><td colspan="2">Como implementar</td></tr>
<tr><td colspan="2">❖ Definir el formato o documento en el cual se solicite a cada una de las áreas el listado de funcionarios y proveedores.</td></tr>
<tr><td colspan="2">❖ Consolidar el listado, clasificándolo por consumidores y proveedores.</td></tr>
<tr><td colspan="2">❖ Para cada uno establecer lo siguiente:
<u>Consumidores:</u>
✓ Procesos y/o actividades que realiza.
✓ Sistemas o Servicios de información que utiliza.
✓ Impacto de los servicios en su proceso (alto, medio o bajo).

<u>Proveedores:</u>
✓ Tipo de Proveedor (Critico o no critico)
✓ Listar cada uno de los servicios que presta, estableciendo si son servicios en la nube, internet u otro y describiendo cada uno, e identificando si el servicio se brinda en la compañía con las herramientas de la misma o en las instalaciones del proveedor.
✓ Procesos que soporta.</td></tr>
</table>

Numeral 8 - Activos en el Ciberespacio	
Objetivos	Identificar cada uno de los activos con los que cuenta la organización.
Requerimiento	Un activo es algo que tiene valor para un individuo o una organización. Hay muchos tipos de activos, incluyendo pero sin limitarse a: a) la información; b) software, como un programa de computador; c) físico, tal como un computador; d) los servicios; e) las personas, sus cualificaciones, habilidades y experiencia, y f) los activos intangibles, como la reputación y la imagen. Para los fines de esta norma nacional, los activos en el Ciberespacio se clasifican en las siguientes clases: ❖ Personal ❖ Organizacional. Para ambas clases, un activo también puede ser clasificado como: ❖ un activo físico, cuya forma existe en el mundo real ❖ un activo virtual, que solo existe en el Ciberespacio y no se puede ver o tocar en el mundo real. Activos personales Uno de los activos virtuales claves es la identidad en línea de un consumidor individual y su información de crédito en línea. La identidad en línea se considera un activo, ya que es el identificador clave para cualquier consumidor individual en el Ciberespacio. Otros activos virtuales individuales de los consumidores incluyen referencias en los mundos virtuales. En los mundos virtuales, los miembros a menudo usan sus avatares virtuales para presentarse o identificarse a sí mismos, o para actuar a su nombre. A menudo, una moneda virtual se utiliza para las transacciones virtuales. Estos avatares y la moneda pueden

	ser considerados como activos pertenecientes a un consumidor individual.

Como implementar

- ❖ Identificar lo siguiente:
    a. ¿Qué información es necesaria para la ejecución del proceso y/o servicio?
    b. ¿Cuáles son las aplicaciones requeridas para gestionar esta información?
    c. ¿Dónde están alojadas estas aplicaciones?
    d. ¿Dónde se almacena la información?
    e. ¿Estas aplicaciones dependen o son administradas por un tercero?
    f. ¿La información es transmitida por red local o por medio de internet?

- ❖ Realizar un inventario de cada uno de los activos teniendo en cuenta lo siguientes:
    a. Nombre del Activo
    b. Procesos a los cuales está asociado
    c. Categoría del activo: Servicio, Hardware, Software, Personas, otros.
    d. Ubicación del activo: Físico – Virtual.
    e. Tipo: Propio o Tercerizado.
    f. Criticidad: Alto, Medio o Bajo.
    g. Activos de los que depende.
    h. Esta incluido dentro del Plan de Continuidad del Negocio.
    i. Valor del activo de acuerdo a confidencialidad, disponibilidad o integridad.

* Escala de calificación de 1 a 4 donde:

1: La pérdida no impedirá la continuidad de la operación.

2: La pérdida causara un impacto bajo en la operación.

3: La pérdida causara un impacto medio en la operación.

4: La pérdida causara un impacto alto en la operación.

- ❖ Validar lo establecido en el numera A8 – Gestión de Activos del anexo 1 de la norma ISO 27001 – 2015.

Numeral 9 - Amenazas contra la seguridad del ciberespacio	
Objetivos	Identificar las amenazas a las cuales tan expuestos en el Ciberespacio.
Requerimiento	Las amenazas que existen en el Ciberespacio se abordan en relación a los activos en el Ciberespacio. Las amenazas al Ciberespacio se pueden dividir en dos áreas clave: ❖ Las amenazas a los activos personales; ❖ Amenazas a los activos de la organización; Amenazas para los activos personales Las amenazas a los bienes personales giran principalmente en torno a cuestiones de identidad, planteadas por la fuga o robo de información personal. Amenazas a los activos organizacionales La presencia de las organizaciones en línea y los negocios en línea a menudo son el objetivo de malhechores cuya intención es más que una simple travesura. Los agentes de amenazas Un agente de amenaza es un individuo o grupo de individuos que tienen algún rol en la ejecución o apoyo de un ataque. Vulnerabilidades La evaluación de las vulnerabilidades debe ser una tarea permanente. Mientras los sistemas reciben parches, se añaden actualizaciones o nuevos elementos, nuevas vulnerabilidades se pueden introducir. Mecanismos de ataque Los ataques pueden provenir de dos categorías principales:

<table>
<tr><td></td><td>❖ Ataques desde el interior de la red privada, y
❖ Ataques desde fuera de la red privada.</td></tr>
<tr><td colspan="2">Como implementar</td></tr>
<tr><td colspan="2">Amenazas</td></tr>
<tr><td colspan="2">❖ Generar y/o tomar como referencia algún catálogo de amenazas mediante las cuales se pueden establecer o identificar las mismas, para ello pueden tomar como referencia la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, del Ministerio de Hacienda y Administraciones Públicas de España: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html</td></tr>
<tr><td colspan="2">❖ Tomando el inventario realizado en el ítem 8, identificar para cada uno las amenazas a las cuales se ven expuestos los activos, de acuerdo al catálogo definido como referencia., adicionalmente identificar vulnerabilidades clasificándolas entre físicas y lógicas.</td></tr>
<tr><td colspan="2">❖ Identificar los servicios y/o aplicaciones que están expuestas en el ciberespacio y allí establecer las vulnerabilidades a las amenazas a las cuales se ven expuestos y los impactos que esto genera.</td></tr>
<tr><td colspan="2">❖ Para cada una de las amenazas identificadas los individuos que podrían generar el ataque (Empleado, Exempleado, hacker, otro)</td></tr>
<tr><td colspan="2">❖ Para cada una de las amenazas establecer los niveles de impacto, para los cuales se puede tomas como referencia el siguiente esquema de calificación:
<table>
<tr><th rowspan="2">Degradación de la Amenaza</th><th colspan="4">Valor de la dimensión del activo</th></tr>
<tr><th>0</th><th>1</th><th>2</th><th>3</th></tr>
<tr><td>0 – Sin degradación.</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td>1 – Degradación Baja</td><td>0</td><td>1</td><td>2</td><td>3</td></tr>
<tr><td>2 – Degradación Media</td><td>0</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>3 – Degradación Alta</td><td>0</td><td>3</td><td>4</td><td>5</td></tr>
</table>
De acuerdo a la tabla anterior evaluar cada una de las amenazas de acuerdo al impacto en los pilares de la información.</td></tr>
</table>

Amenaza	Impacto Confidencialidad	Impacto Integridad	Impacto Disponibilidad

Vulnerabilidades

- Para cada uno de los procesos identificar las Vulnerabilidades en el Ciberespacio relacionadas con la actividad que desarrollan en sus labores diarias.
- Para cada una de las amenazas identificadas establecer las vulnerabilidades a las cuales se ve expuestas.
- Para las vulnerabilidades técnicas, ejecutar un análisis de vulnerabilidades por parte de un tercero para los canales y sistemas de información que permitan generar controles y llevar un inventario de vulnerabilidades, que permita identificar cuales cuentan con control y/o cuales requieren un tratamiento por parte de la compañía para mitigar riesgos que afecten la continuidad del negocio.
- Contar con inscripciones a bases de vulnerabilidades y/o amenazas de tal forma que se pueda alimentar el inventario, para que sean evaluadas y se implemente una solución efectiva.
- Clasificar las vulnerabilidades identificadas de acuerdo a la criticidad del activo evaluado a fin de establecer una prioridad para la implementación de controles.
- Para la gestión de las vulnerabilidades tomar como referencia el Anexo 12.6 - Gestión de la vulnerabilidad técnica del Anexo A de la ISO 27001 y responder a las siguientes preguntas:
    a. ¿Existe una política la gestión de vulnerabilidades técnicas?
    b. ¿Cómo se escanean los sistemas para detectar vulnerabilidades de forma automatizada?
    c. ¿Cómo responde la organización ante vulnerabilidades técnicas descubiertas en equipos, servidores, aplicaciones, dispositivos de red y otros componentes?
    d. ¿Existen procesos adecuados para verificar los inventarios de los sistemas e identificar si las vulnerabilidades divulgadas son relevantes?
    e. ¿Se identifican cambios tales como amenazas emergentes, vulnerabilidades conocidas o sospechadas, y consecuencias o impactos comerciales en evolución?
    f. ¿Los parches son evaluados por su aplicabilidad y riesgos antes de ser implementados?
    g. ¿Los procesos para implementar parches urgentes son adecuados?

h. ¿Existen registros de aprobación o rechazo de implementación de parchas asociado a vulnerabilidades (aceptación de riesgo) en los niveles de administración adecuados?
❖ Para cada una de las herramientas que están en el ciberespacio, identificar: a. Medios de conexión: Red Local, Internet (hogar, Aeropuertos), red móvil, otros. b. De acuerdo a la criticidad identificada en el inventario de activos, realizar para cada una de las herramientas desde la más crítica a la de menos impacto, las conexiones más usadas entre los colaboradores e identificar los ataques a los cuales se puede ver expuestos y los controles que a la fecha están implementados para este tipo de ataques.
✓ Evaluar la implementación de un correlacionador de eventos, como un SIEM (Security Information and Event Management) o un SOC (Security Operation Center) mediante los cuales puede monitorear y detectar de manera oportunas vulnerabilidades que afecten los sistemas y/o información. Circular Externa 007/18 – Superfinanciera de Colombia.

Numeral 10 - Roles de las partes interesadas en la Ciberseguridad.	
Objetivos	Definir los roles que desempeñan cada una de las partes interesadas.
Requerimiento	Para mejorar el estado de la Ciberseguridad, las partes interesadas en el Ciberespacio tienen que desempeñar un rol activo en su respectivo uso y desarrollo de Internet. Estos roles pueden a veces sobreponerse con sus roles individuales y organizacionales dentro de sus redes personales o de la organización.
Como implementar	
❖ Para cada una de las partes interesadas identificadas en el numeral 7, se deben establecer los roles, teniendo en cuenta la incidencia que tienen dentro de la operación, es decir qué tipo de actores son dentro del proceso, directos o indirectos.	
❖ Tomar como referencia las planteadas en el numeral 10 de la ISO27032, como son: Los **roles de los consumidores** pueden incluir, pero no se limitan a, los siguientes: ✓ Usuarios de aplicaciones generales del Ciberespacio o usuario general, como un reproductor de juego en línea, el usuario de mensajería instantánea, o internauta;	

- ✓ Comprador/vendedor, que participa en la colocación de productos y servicios en sitios de subastas en línea y del mercado para los compradores interesados y viceversa;
- ✓ Blogger y otro contribuyente de contenidos (por ejemplo, un autor de un artículo en un wiki), en el que la información de texto y multimedia (por ejemplo, clips de vídeo) se publican para público en general o el consumo de un público limitado;
- ✓ Proveedor independiente de aplicaciones (IAP) dentro de un contexto de aplicación (por ejemplo, un juego en línea), o en el Ciberespacio en general;
- ✓ Miembro de una organización (por ejemplo, un empleado de una empresa, u otra forma de asociación con una empresa);
- ✓ Otros roles. Es posible que a un usuario se le pueda asignar un rol involuntariamente o sin su consentimiento.

Roles de las organizaciones

Las organizaciones a menudo utilizan el Ciberespacio para publicitar a la empresa y la información relacionada, así como productos y servicios relacionados con el mercado. Las organizaciones también utilizan el Ciberespacio como parte de su red para la entrega y la recepción de mensajes electrónicos (por ejemplo, mensajes de correo electrónico) y otros documentos (por ejemplo, transferencia de archivos).

- ➢ Validar los lineamientos que presenta la norma ISO27032 – numeral 10, para la identificación de los roles de acuerdo a tipo de partes interesadas.

Numeral 11 - Directrices para los interesados	
Objetivos	Establecer los lineamientos para definir los directrices para las 3 áreas principales que presenta el numeral 11.
Requerimiento	La orientación en este capítulo se centra en tres áreas principales: ❖ Orientación de seguridad para los consumidores ❖ La gestión de riesgos de seguridad de la información interna de una organización. ❖ Los requisitos de seguridad que los proveedores deberán especificar para que los consumidores apliquen.

Como implementar
De acuerdo a los lineamientos que presenta la norma, para la implementación de este numeral, iniciaremos por la evaluación y tratamiento de riesgos, para lo cual se debe tener en cuenta lo siguiente: a. Elegir una metodología para la identificación y evaluación de riesgos. b. Validar el estándar ISO 31000, en el cual se presentan principios y directrices genéricas sobre la gestión de riesgos. c. Verificar la ISO/IEC 27005, – Gestión de riesgos de seguridad de la información, la cual proporciona directrices y procesos para la gestión de riesgos de seguridad de la información en una organización.
❖ De acuerdo a la metodología de riesgos establecer la matriz de calificación de riesgos.
❖ Tener en cuenta las consideraciones que presenta el numeral 11 de la ISO27032 para la evaluación e identificación de riesgos que permitirán establecer controles para la administración de Ciberseguridad de la organización.
❖ Partiendo del inventario de activos donde se identificaron los activos junto con sus amenazas y vulnerabilidades, identificar los riesgos a los cuales se ven expuestos estos activos, estableciendo el factor que los genera (Personas, Procesos, Sistemas, otros), identificando a que parte interesada pertenecen a fin de establecer si es interno o externo, de tal forma que se puede establecer una causa raíz e impacto, a fin de clasificarlos y dar prioridad para el tratamiento de riesgos.
❖ Validar la Circular Externo 005 de 2019 de la Superfinanciera de Colombia, a fin d identificar los lineamientos a tener en cuenta cuando se tiene información en la nube, de tal forma que se identifiquen riesgos a los cuales se ven expuestos en estos entornos.
❖ Para cada una de las partes interesadas que se identificaron en el numeral 10, se debe realizar una evaluación de riesgos, para ello se puede tomar como referencia la metodología seleccionada para la evaluación de activos, pero se debe tener en cuenta los roles que desempeñan dentro de la organización, si es proveedor o consumidor, los servicios que soportan (Misionales o no misionales). Adicionalmente puede validar los lineamientos que presenta la norma ISO27032 – numeral 10, para la identificación de riesgos respecto a las partes interesadas, a fin de garantizar que se contemplan todos los aspectos de Ciberseguridad, que podrían llegar a impactar el negocio

en caso de materializarse algún riesgo.
❖ Validar los lineamientos que contiene la Circular Externa 007 de 2018 de la Superfinanciera, la cual presenta aspectos a tener en cuenta para la el monitoreo, reporte de incidentes, bases de conocimiento, los cuales permitirán identificar riesgos que estén asociados a la organización o al mercado en el cual se desarrolla.

Numeral 12 – Controles de Ciberseguridad	
Objetivos	Establecer lineamientos para el diseño de los controles que permitirán mitigar los riesgos identificados.
Requerimiento	Una vez que los riesgos de Ciberseguridad se identifican y se redactan lineamientos apropiados, los controles de Ciberseguridad que soportan a los requisitos de seguridad pueden seleccionarse e implementarse. Este capítulo proporciona una visión general de los controles clave de Ciberseguridad que pueden ser implementados para apoyar a los lineamientos establecidos en esta norma nacional.
Como implementar	
❖ Para la implementación de controles, se debe tener en cuenta las aplicaciones, infraestructura como servidores, usuarios finales, proveedores entre otros, para los cuales se identificaron roles y riesgos en los numerales anteriores (7-11).	
Para implementar controles se debe iniciar por definir políticas que regulen la creación, recolección, almacenamiento, trasmisión, distribución, procesamiento, y uso general de la información de la Compañía que sea compartida o administrada en el Ciberespacio, las cuales contengan lineamentos como: ➢ Actualizaciones de seguridad. ➢ Lineamientos para la clasificación y categorización adecuada de la información que se maneja en cada uno de los procesos. ➢ Capacitación y concientización de manera periódica a fin de que todas las partes interesadas tengan conocimiento de los riesgos a los que se exponen al realizar un mal manejo de la información y/o servicios utilizados para sus actividades, de tal forma que en caso de un incidente sean conscientes de las implicaciones y no se amparen en	

desconocimiento. Asegurando que cada uno conoce las funciones y responsabilidades en el Ciberespacio y estar actualizados con las nuevas tendencias o ataques que van generándose constantemente.

- Evaluaciones para cada uno de los desarrollos que involucren las aplicaciones que están en el ciberespacio.
- Monitoreos a los accesos, tanto a las aplicaciones y/ servidores.
- Monitoreos a la información que viaja desde y hacia la aplicación.

❖ Para la definición e implementación de controles se debe tener en cuenta, los siguientes aspectos que presenta la norma dentro de sus controles de Ciberseguridad:

b. Aplicaciones:

- De acuerdo a la información que se identificó en el numeral 7, establecer controles que protejan los datos que son compartidos en línea mediante las aplicaciones, teniendo en cuenta la criticidad para cada uno de los procesos.
- Asegurar el manejo de sesiones para las aplicaciones web.
- Dentro de los desarrollos propios o realizados por terceros establecer lineamientos para la validación a fin de garantizar que son desarrollos seguros, mitigando ataques de inyección de código, huecos de seguridad como Cross-site, Scripting, Visching entre otros, que permitan robo o fuga de información crítica para la Compañía.

c. Servidores:

- Establecer mecanismos de autenticación que mitiguen el acceso a usuarios no autorizados.
- Implementar mecanismos de análisis para la información que es alojada o guardada en los servidores a fin de mitigar software malicio que pueda afectar o comprometer los datos que se alojan allí.
- Definir e implementar mecanismos para el monitoreo de los sistemas a fin de identificar vulnerabilidad, así como la instalación de parches o actualizaciones publican periódicamente Microsoft o generan los proveedores de los sistemas y que mitigan fallas de seguridad identificadas en los mismos.

d. De acuerdo a la información que se identificó en el numeral 7, establecer controles que

protejan los datos que son compartidos en línea mediante las aplicaciones, teniendo en cuenta la criticidad para cada uno de los procesos.

e. Identificar y establecer controles para cada uno de los dispositivos o mecanismos de conexión a la red, minimizando amenazas que se pueden generar a partir del uso de Redes inalámbricas públicas o que no cuentan con mecanismos de seguridad adecuados, bluethooth, voz IP, entre otros.
f. Para la información, establecer controles de acuerdo a la categorización definida por cada uno de los procesos, a fin mitigar la exposición accidentar al o acceso no autorizado a la misma.

Como apoyo para la implementación de controles se recomienda validar los lineamientos que presenta la norma ISO27032 en su numeral 12 y que se detallaron de manera general en esta guía, adicionalmente tomar como referencia el anexo A de la ISO27001, Circular Externa 029 de 2014 de la Superfinanciera de Colombia – Titulo II la cual establece mecanismos para el aseguramiento de canales y medios, Titulo IV Capitulo 5 donde se presentan Requerimientos mínimos para la gestión de la seguridad de la información y la Ciberseguridad, buenas prácticas como COBIT u otras les permitirá establecer controles efectivos para la mitigación de riesgos que afecten la continuidad de las operaciones, entre otras apliquen de acuerdo al negocio.

Numeral 13 – Marco de intercambio y Coordinación de la información.	
Objetivos	Identificar los lineamientos a tener en cuenta para el intercambio de información en el ciberespacio.
Requerimiento	Es necesario establecer un sistema para el intercambio y coordinación de la información que ayude a preparar una respuesta a los eventos e incidentes de Ciberseguridad. Este es un paso importante que las organizaciones deberían dar como parte de sus controles de Ciberseguridad. Un sistema tal para el intercambio y la coordinación de la información debería ser seguro, eficaz, fiable y eficiente.
Como implementar	
❖ Para la implementación de este numeral la norma presenta unas condiciones a tener en cuenta, las cuales se detallan a continuación:	

a. De acuerdo a la información recolectada en los ítems anteriores, identificar qué información se recibe y/o envía en el ciberespacio, estableciendo que medios se utilizan para ello (aplicación, FTP, WEB, otro) que categorización tiene la información (Alta, media, baja, confidencial, publica, otros).
b. Teniendo en cuenta lo anterior, identificar los riesgos, amenazas, vulnerabilidad y otros elementos asociados a cada tipo de información y medio utilizado para el intercambio de la misma, a fin de establecer los aspectos en los cuales se pueda ver comprometida la información que se comparte en el ciberespacio.
c. Realizar la evaluación de riesgos, de acuerdo a la metodología seleccionada por la compañía, a fin de identificar los más críticos, de tal forma que se generen controles que permitían mitigar impactos jurídicos, financieros u otros para la misma.
d. Identificar políticas o normas para el tratamiento de esta información, por ejemplo: Ley de protección de datos personales, a fin de contemplar medidas a tener en cuenta para la transmisión de información desde y hacia otros, mediante canales.
e. A nivel de intercambio de información consultar el Título V – "Protección de Datos Personales" de la Circular Unica de la Superintendencia de industria y comercio, la cual en su Capítulo III menciona los países con los cuales recomiendan la transferencia de datos personales, los cuales pueden tomarse como referencia a la hora de evaluar la transferencia de información.

Con cada uno de los lineamientos definidos para los diferentes numerales de la ISO 27032, que se plantearon en las tablas anteriores y la metodología propuesta, las organizaciones tienen un elemento base para la implementación de esta buena práctica, enfocándose en los aspectos críticos o menos fortalecidos, donde pueden estar más expuestos, adicionalmente para la implementación de este sistema de gestión es importante tener en cuenta los siguientes aspectos:

- ✓ Los procedimientos, políticas u otros siempre deben de estar apoyados por la alta dirección para que estos sean adoptados por cada uno de los integrantes de la organización.

- ✓ Revisar la ISO27003 para identificar otros lineamientos y/o aspectos a tener en cuenta para la implementación de un sistema de Gestión.
- ✓ Evaluar la relación entre objetivos estratégicos y alineación con el negocio que presenta COBIT 2019, para la implementación de controles.
- ✓ Evaluar los contratos establecidos con terceros que administran la infraestructura y/o aplicaciones, de tal forma que estos cuenten con cláusulas o requisitos a cumplir para la administración de la información, de tal forma que se mitiguen riesgos de incumplimiento respecto a la transferencia de información.
- ✓ Consultar la metodología MARGERIT la cual presenta un enfoque para la evaluación de riesgos de TI, respecto a los activos de información.
- ✓ Consultar la NIST de Ciberseguridad la cual ofrece lineamientos para la identificación, protección, detección, respuesta los cuales pueden ser aplicados en cada uno de los numerales a implementar de la normal.

5.1.5 APORTE DE LOS RESULTADOS A LA SEGURIDAD DE LA INFORMACIÓN

Una vez conocida la situación actual y el nivel de protección que brinda la legislación colombiana a los datos que tanto los ciudadanos colombianos como las empresas exponen en el ciberespacio, se logró evidenciar la falta de protección que tienen los activos de información, dado que con los avances tecnológicos los entornos físicos de TI se han convertido en virtuales y no son administrados directamente por las organizaciones, esto debido a que no se cuentan con los conocimientos y/o experticia necesaria para la implementación de controles que permitan asegurar los datos y/o información que es parte fundamental y uno de los activos más críticos para las organizaciones.

Los aportes que realiza este trabajo de investigación a la seguridad de la información están encaminados a mostrar los lineamientos a tener en cuenta para asegurar cada uno de los activos que tiene la organización en el ciberespacio mediante la implementación de las buenas prácticas definidas en la ISO 27032.

5.1.6 CÓMO SE RESPONDE A LA PREGUNTA DE INVESTIGACIÓN CON LOS RESULTADOS

Los lineamientos definidos en el capítulo 5, permitirán a una organización sin importar el tipo de negocio y/o tamaño, generar un diagnostico en el cual evidencien el estado de la misma respecto al riesgo de Ciberseguridad. Respondiendo a la pregunta de investigación, es posible afirmar que la guía definida para la implementación de las buenas prácticas que presenta la ISO27032, generara a las organizaciones elementos o directrices para implementarla, de tal forma que se minimice el impacto de los riesgos a los cuales están expuestos sus activos de información y de esta forma estar preparados para responder de manera más efectiva a un incidente. A esta respuesta se llega, después de validar y analizar el estado de los ciberataques en el país y evaluar cada una de las directrices que presenta la ISO para contrarrestar a los impactos que estos pueden ocasionar en una organización.

5.1.7 ESTRATEGIAS DE COMUNICACIÓN Y DIVULGACIÓN

El presente proyecto de investigación se divulgará a través de una socialización frente a los jurados asignados para tal fin, y se encontrará disponible en el repositorio de la biblioteca de la Universidad Católica de Colombia.

6 CONCLUSIONES

En esta investigación se diseñó una guía mediante la cual las organizaciones realicen la implementación de las buenas prácticas de ISO 27032, realizando la identificación de los requerimientos que presenta esta norma, iniciando con el inventario de activos, luego evaluando los riesgos de tal forma que se generen controles que mitiguen las amenazas a las cuales se ve expuesta la información en el ciberespacio y que pueden llegar a afectar la continuidad de su operación.

La aplicación de la guía presentada en esta investigación permitirá a las organizaciones identificar el estado en el que se encuentran a nivel de Ciberseguridad, e implementar controles sobre puntos que claves para la organización, tomando como base lo planteado en esta investigación.

Resultado de la investigación, se puede concluir que en Colombia muchas de las Compañías hoy en día cuentan con un gran porcentaje de información en el ciberespacio, sin embargo no existen lineamientos que les permita asegurar esta información de manera efectiva y eficiente, a excepción del sector financiero que por su regulación se los exige.

7 BIBLIOGRAFÍA

Andes, U. d. (Mayo de 2018). *Ciberseguridad en la era del internet de las cosas* - . Obtenido de Sistemas Uniandes: https://sistemas.uniandes.edu.co/images/forosisis/revista/8/pdf/FOROS-ISIS-8.pdf

CIS, C. f. (2019). Obtenido de Cybersecurity Best Practices: https://www.cisecurity.org/cybersecurity-best-practices/

Consultores, G. A. (s.f.). *NORMA ISO 27032 GESTIÓN DE LA CIBERSEGURIDAD*. Recuperado el octubre de 2018, de Grupo ACMS Consultores Web site: https://www.grupoacms.com/norma-iso-27032

Edge, T. (Noviembre de 2017). *Gestion_de_riesgos_de_ciberseguridad_basado_en_ISO_27032*. Obtenido de Tactical Edge 2019.

Gomez Fernandez, L., & Fernandez Rivero, P. (2018). *Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad.* AENOR - Asociación Española de Normalización y Certificación.

Gomez Vieites, A. (2013). *Seguridad en Equipos Informaticos* (1 ed.). Bogota, Colombia: Ediciones de la U.

Gómez, F. L., & Rivero, Pedro , P. (2018). *Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad, AENOR - Asociación Española de Normalización y Certificación.* (A. I. S.A.U, Ed.) España: ProQuest Ebook Central. Obtenido de https://ebookcentral.proquest.com/lib/biblioucatolicasp/detail.action?docID=5486388

INCIBE, E. (Agosto de 2018). *Instituto Nacional de Ciberseguridad*. Obtenido de INCIBE - eSPAÑ: https://www.incibe.es

ISO. (2012). *Information technology — Security techniques — Guidelines for cybersecurity.* Switzerland: ISO copyright office.

ISO. (2018). *ISO Survey*. Obtenido de International Organization for Standardization: https://www.iso.org/the-iso-survey.html

ISO/IEC. (2012). *Estandar Internacional ISO/IEC 27032:2012(E).* Switzerland: ISO copyright office.

ISO/IEC. (2013). *ISO 27001 - INFORMATION SECURITY MANAGEMENT*. Switzerland: (ISO/IEC, 2013).

KPMG. (2018). *Building Cyber Resilience in Asset Management.* KPMG International. Obtenido de https://assets.kpmg.com/content/dam/kpmg/bm/pdf/2018/07/building-cyber-resilience-in-asset-management.pdf

MINTIC. (de de 2017). *Micrositios*. Obtenido de ABC de la Digitalización: http://micrositios.mintic.gov.co/abc_digitalizacion_empresas/

Nieva, M., & Gazapo, M. (Octubre de 2016). LA CIBERSEGURIDAD COMO FACTOR CRÍTICO EN LA UNION EUROPEA. *Revista UNISCI*, pág. 68.

NIST. (2019). *National Institute of Standards and Technology*. Obtenido de CYBERSECURITY FRAMEWORK: https://www.nist.gov/cyberframework

Policia, N. d. (2019). Centro Cibernetico Policial. Bogotá. Obtenido de

https://caivirtual.policia.gov.co/

Price Water House, C. (2018). *Ciberseguridad y privacidad: De la percepción a la realidad.* Mexico: PWC.

SIC, S. d. (19 de Julio de 2001). Circular única. Bogotá, Colombia. Obtenido de Superintendencia de Industria y Comercio.

Superfinanciera. (junio de 2018). *Circular Externa 007*. Obtenido de Superintendencia Financiera de Colombia: https://www.superfinanciera.gov.co/publicacion/10096745

Universidad, d. R. (Noviembre de 2017). *Colombia no está preparada ante un ciberataque*. Obtenido de http://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/